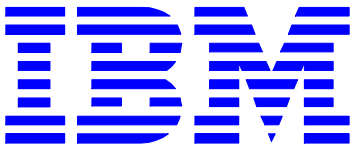


IBM Integration Bus

Broker Administration using the Web Administration Interface

September, 2013

Hands-on lab built at product
code level version 9.0.0.0
Toolkit iFix 1

1. INTRODUCTION 3

1.1 Lab preparation ..... **Error! Bookmark not defined.**

1.2 Reset IB9NODE security 3

2. PREPARE THE IB9NODE APPLICATIONS 4

3. A FIRST LOOK AT THE WEB ADMIN INTERFACE (NO SECURITY) 14

4. CONFIGURE ROLE-BASED SECURITY FOR WEB USERS 18

4.1 Activate security for IB9NODE 19

4.2 Define the MQ authorities for the web users 21

4.3 Define the MQ authorities manually (optional) 22

4.4 Define the web users for IB9NODE 27

5. USING THE WEB ADMIN INTERFACE WITH SECURITY 28

5.1 The web admin interface for a read-only user 28

5.2 The Web Admin interface for a user with update access 33

6. EXPLORING THE WEB ADMIN FLOW STATISTICS FACILITIES 36

6.1 Investigate the statistics function in the web admin interface 36

6.2 Using the Web Admin interface to show running flow statistics 48

6.3 Create and use a policy to limit flow throughput 59

1. Introduction

WebSphere Message Broker Version 8 and 8.0.0.1 introduced the web browser administration tools, and IBM Integration Bus Version 9 has made significant improvements in this function. The Web User Interface (known in this document as the Web UI) provides the following capabilities:

- Ability to define web users (with associated userid/password authentication)
- Ability to allow defined users to perform password and profile maintenance
- Ability to define appropriate levels of authorization for authenticated users (role-based security)
- Ability to perform update actions against deployed resources (start, stop, etc.)
- Ability to view trace and log files through the Web UI
- Ability to view and update broker policy documents
- Ability to create pattern instances and deploy direct to a broker (limited function at the moment)
- Enhanced function specifically for the Record and Replay item, with associated authorization profiles

This lab will demonstrate some of these points, with the exception of the Record/Replay topic. This is the subject of a separate lab.

This lab has been updated for IBM Integration Bus version 9.0, and specifically includes topics covering flow statistics and policy-controlled workload management.

1.1 Reset IB9NODE security

The first part of this lab assumes that security has not been activated for IB9NODE. If security has been activated on your system, deactivate it now:

Set security off with the following commands in an Integration Command Console:

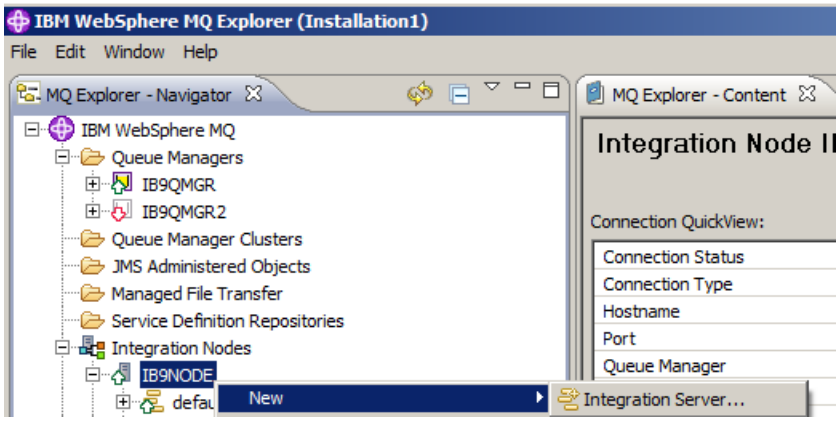
```
mqsistop IB9NODE

mqsichangebroker IB9NODE -s inactive

mqsistart IB9NODE
```

2. Prepare the IB9NODE applications

So that the Web UI has some artefacts on which to operate, you will first deploy some application artefacts.

1. If not already open, start the Integration Bus Explorer (MQ Explorer) from the desktop icon.

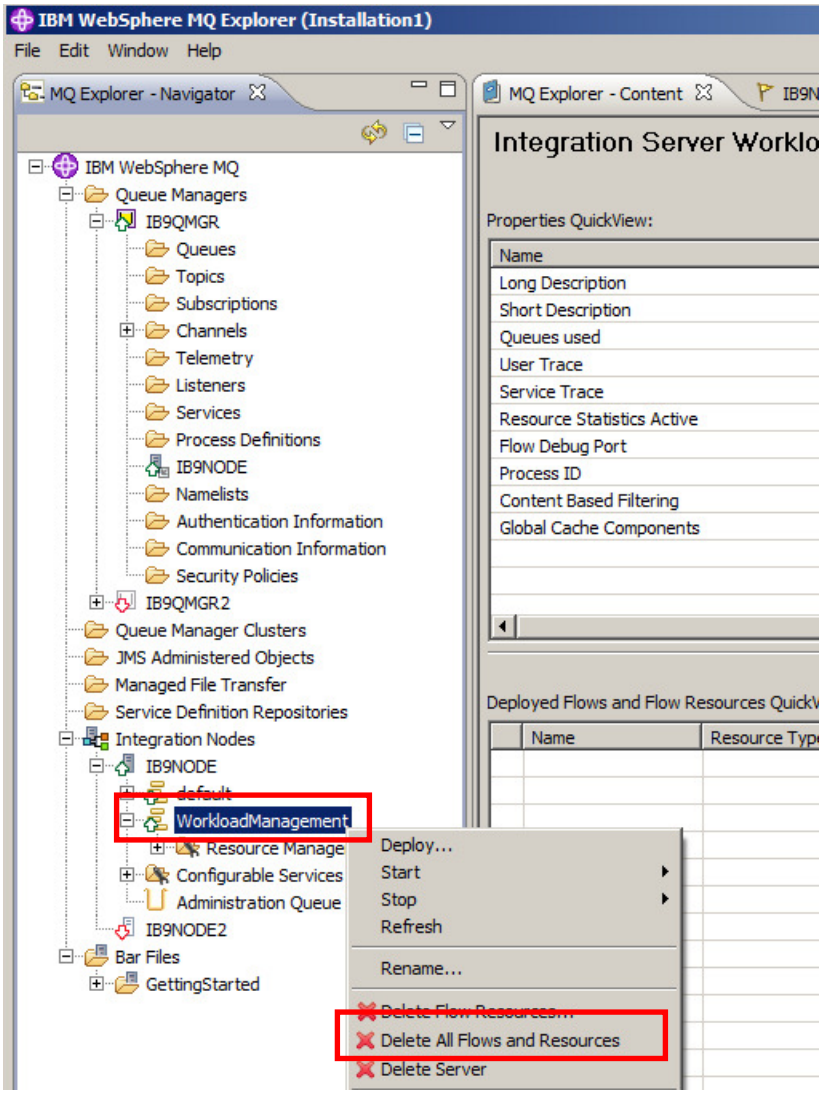
   We will be using the WorkloadManagement integration server (known as an execution group in earlier versions of WebSphere Message Broker). If you do not have the WorkloadManagement integration server, right-click on IB9NODE and select New > Integration Server, and name it WorkloadManagement (correct case).



   Click OK.

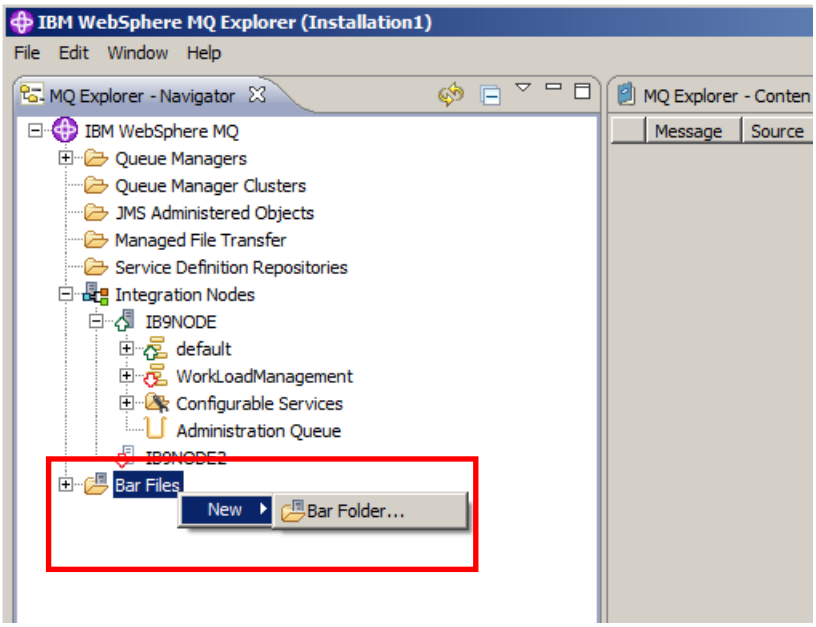
2. If you have done the WorkloadManagement labs, you may already have resources deployed in this server. We want to deploy fresh copies of the message flows to the integration server, so we will delete any current resources.

   In the Integration Nodes pane, right click the WorkloadManagement integration server and select Delete > All Flows and Resources.

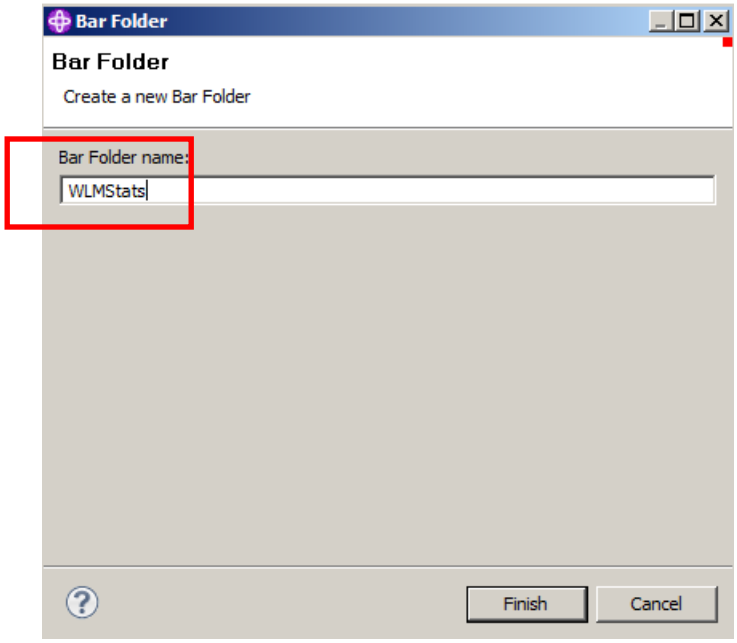


3. Still in the Integration Bus Explorer (not the toolkit), deploy the barfiles for testing the Web UI interface. First, import the BAR files into the Explorer.

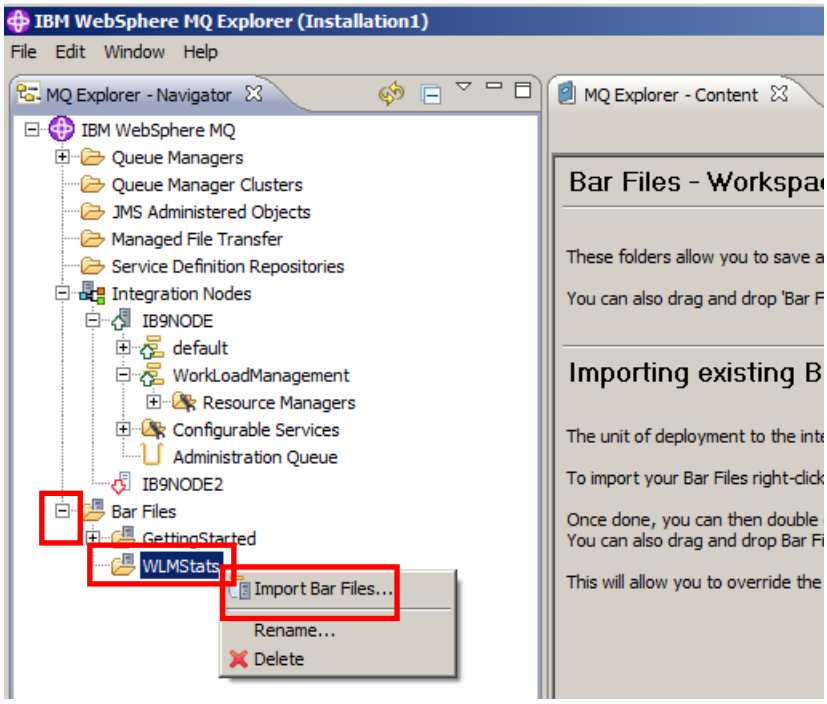
   Right-click Bar Files, select New > Bar Folder.



   In Bar Folder name, type in WMLStats.
   Click Finish.

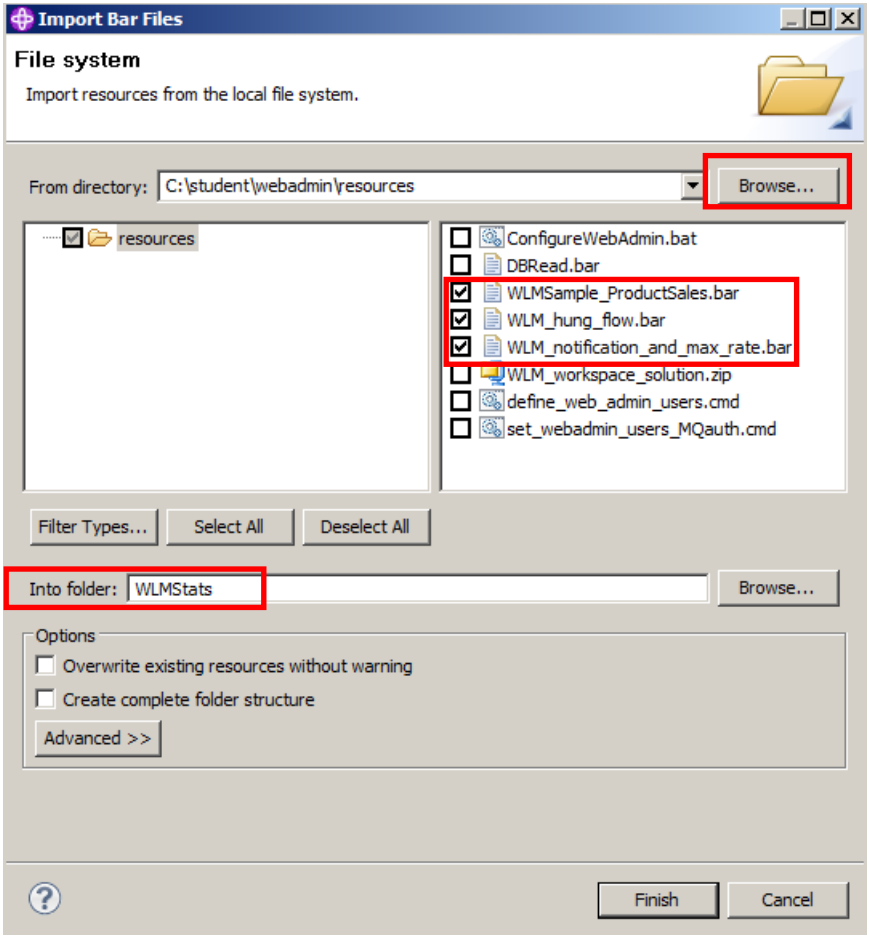


4. Right click WLMStats and select Import Bar Files.

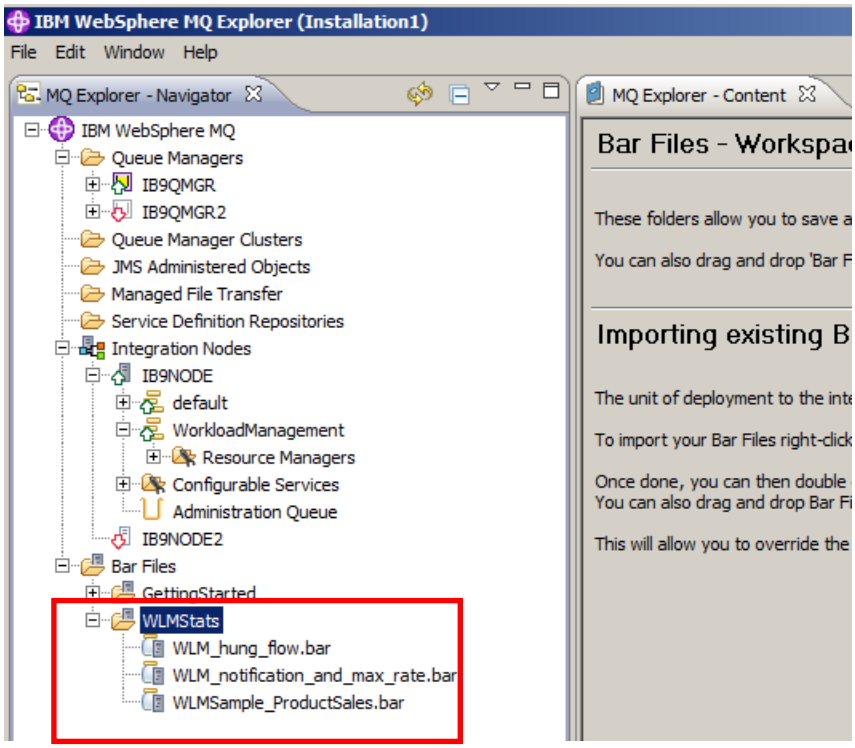


5. On the Import Bar Files panel, click Browse and navigate to C:\student\webadmin\resources.

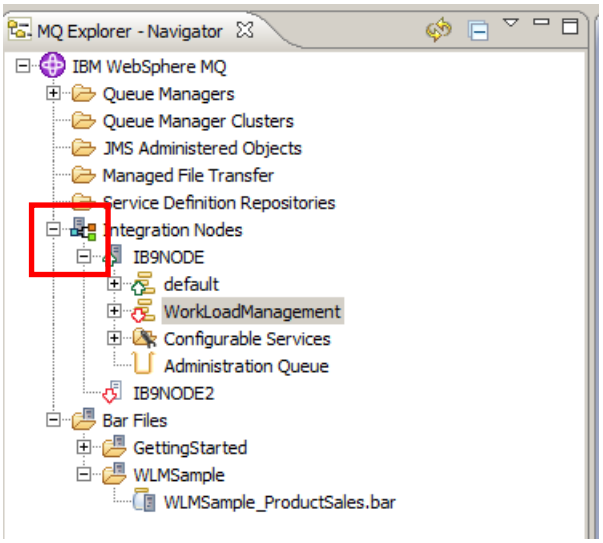
   Tick the check boxes for WLMSample_ProductSales.bar, WLM_hung_flow.bar, and WLM_notification_and_max_rate.bar.



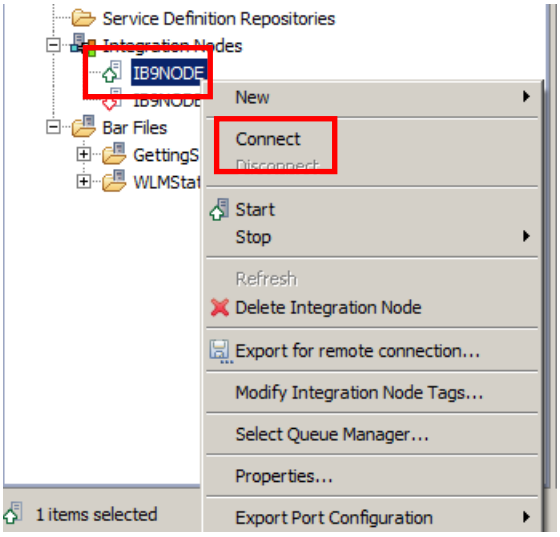
6. Your Bar Files folder should now contain the BARs we need to produce statistics later in the lab.



7. Expand the Integration Nodes and IB9NODE.

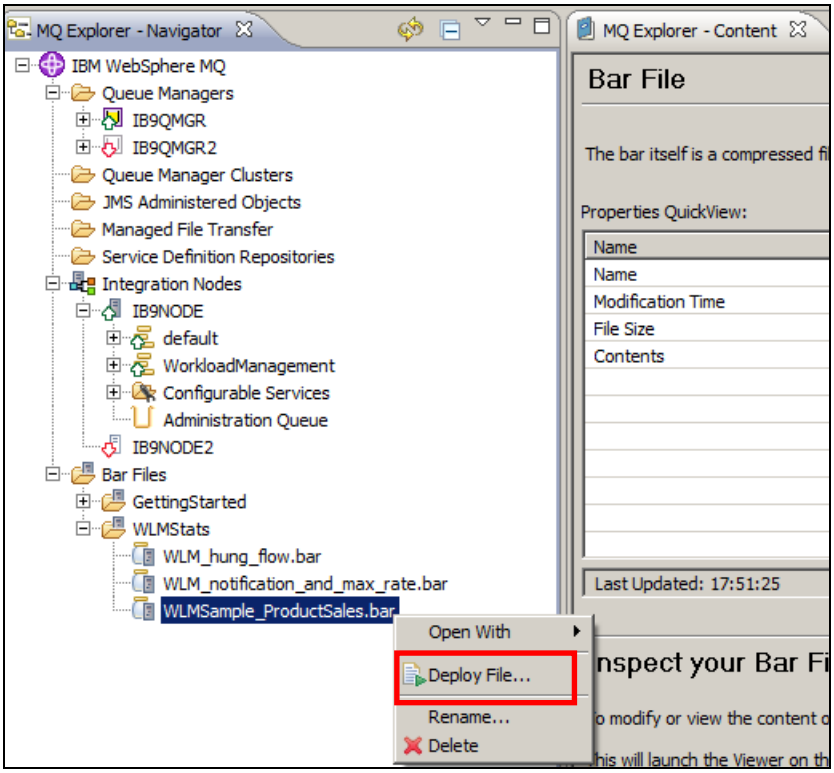


If you do not see any Integration Servers under IB9NODE, right-click it and select Connect.

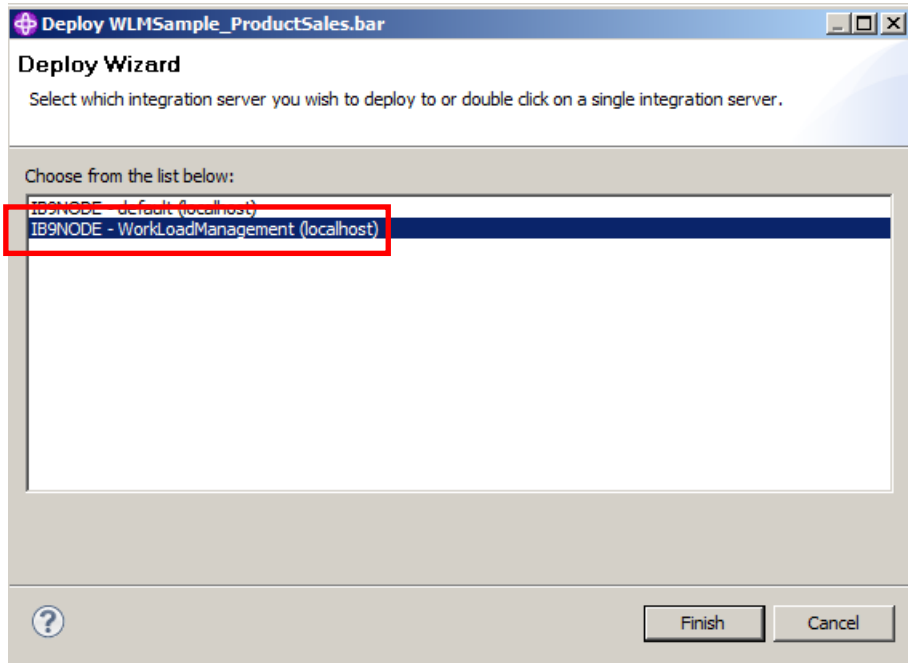


If the WorkLoadManagement integration server is not started, right-click it and select Start.

8. Expand the WLMStats folder, right-click WLMSample_ProductSales.bar and select Deploy File.



On the Deploy Wizard, select IB9NODE – WorkLoadManagement (localhost) and click Finish.



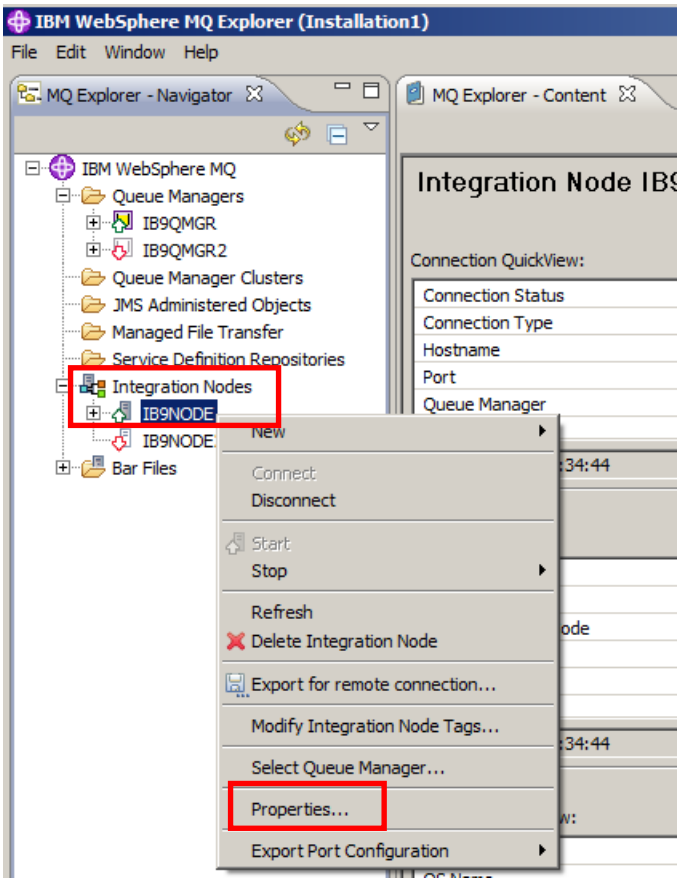
The BAR is deployed to the WorkLoadManagement integration server.

9. Repeat step 8 for the other two barfiles.

   You now have running flows for exercising the Web UI and displaying message flow statistics later in the lab.

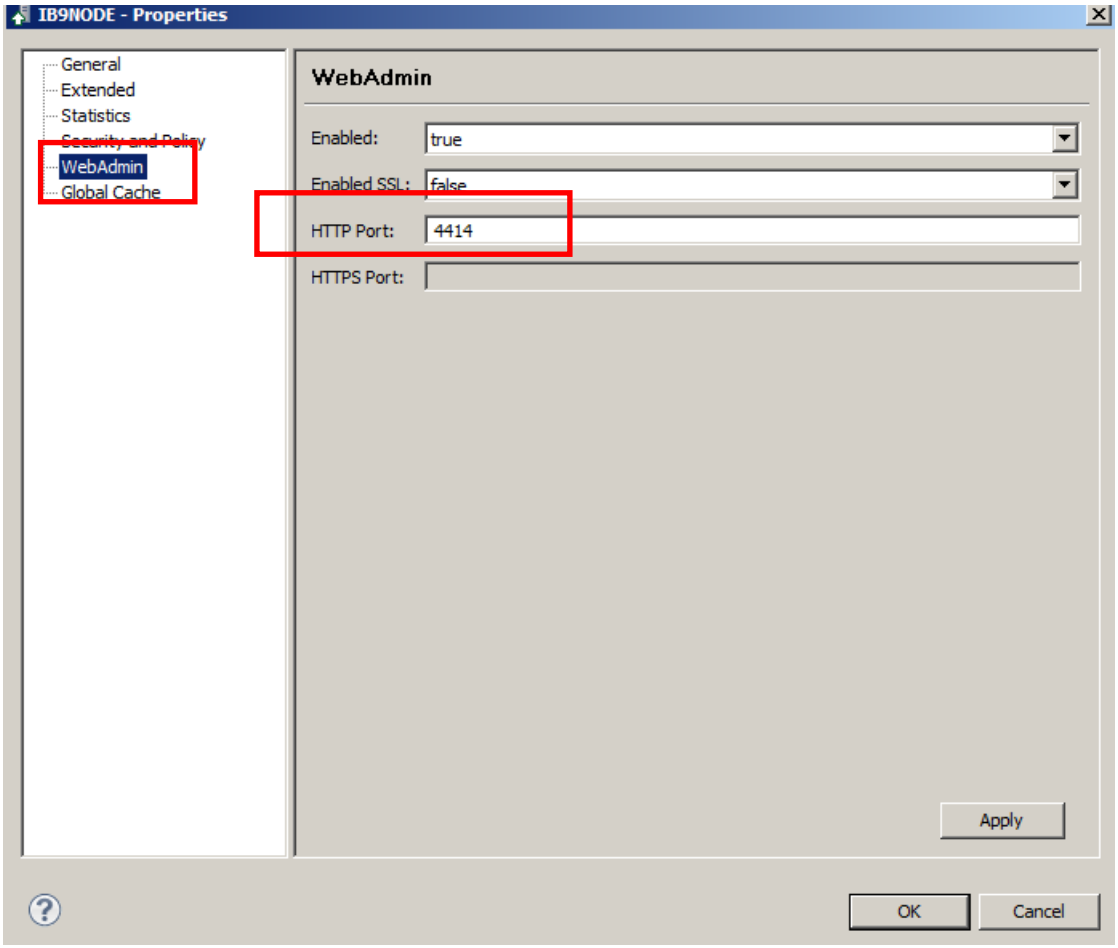
10. In IB Explorer, specify the HTTP listener for the Web Admin UI.

    Right-click IB9NODE, and select Properties.



11. Select WebAdmin. The WebAdmin listener is already started by default, and has been set to the default port value of 4414 (registered with the IANA). You can leave all values unchanged.

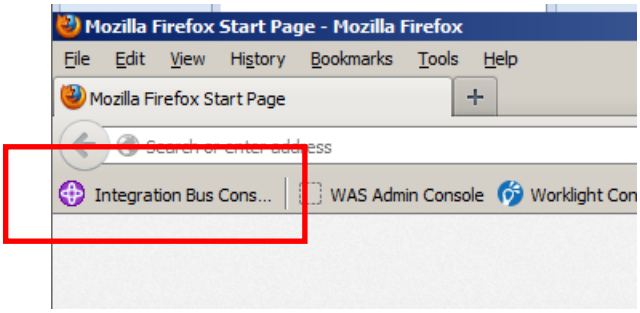
    Click OK.



3. A first look at the Web Admin Interface (no security)

1. Open a Firefox web browser by double-clicking the desktop icon.

   Click the provided shortcut link, Integration Bus Console (http://localhost:4414).

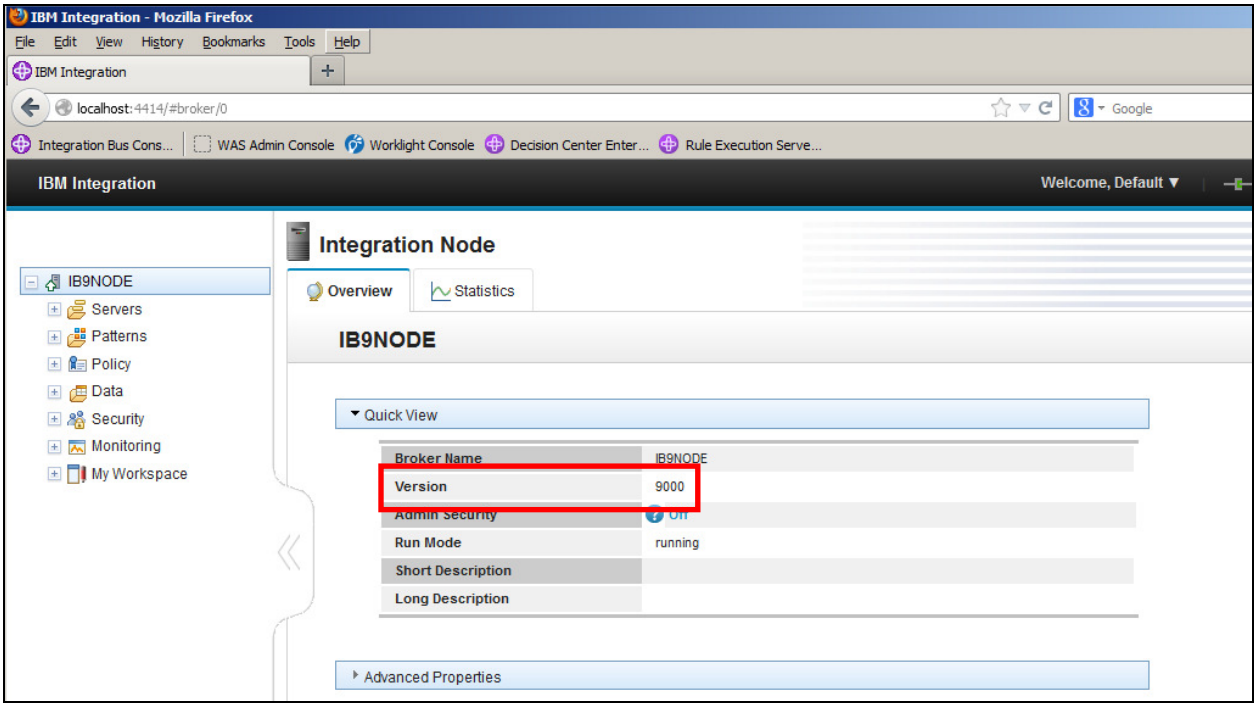


2. You will immediately note that you are logged in automatically, using the default user.

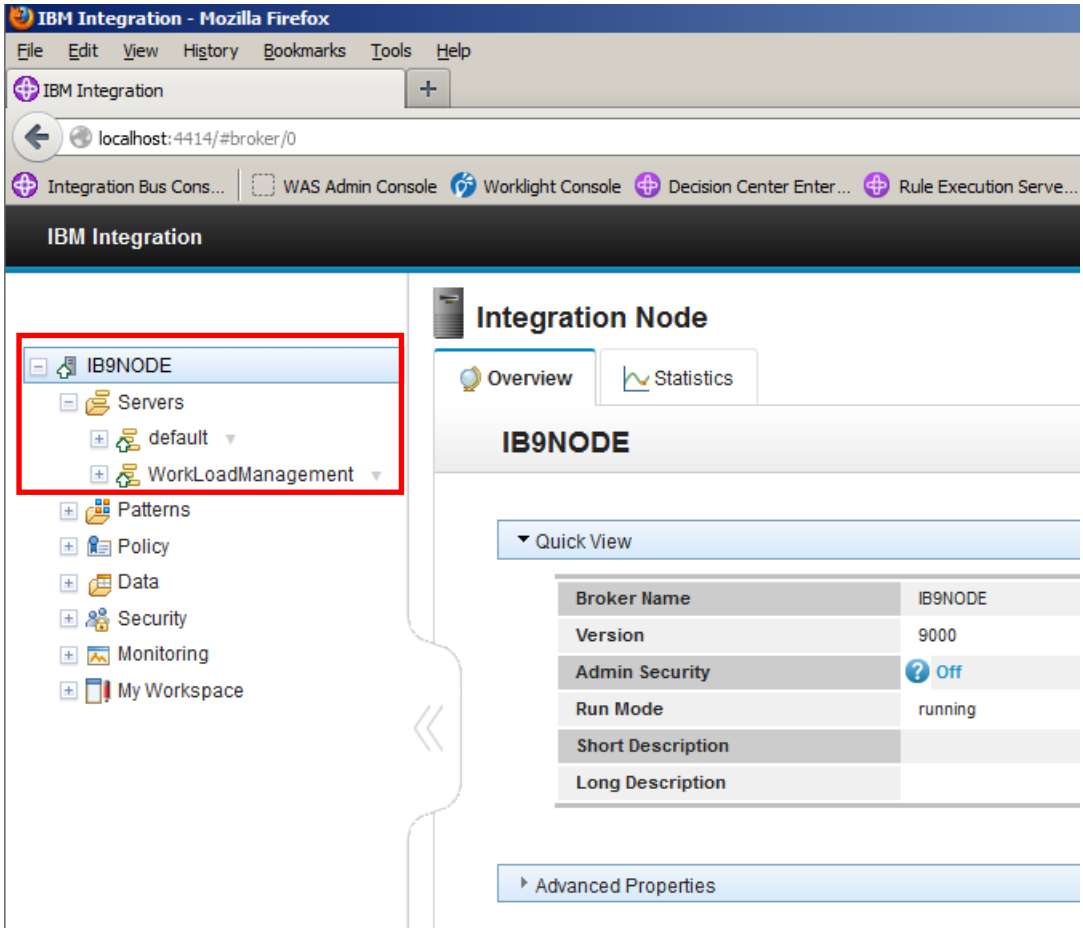
   Note that Admin Security is off.

   In this scenario, the default user has full update access to all deployed broker resources.

   If you have enabled the web admin http listener, and have defined web users, then you should fully enable security on systems that need such protection.

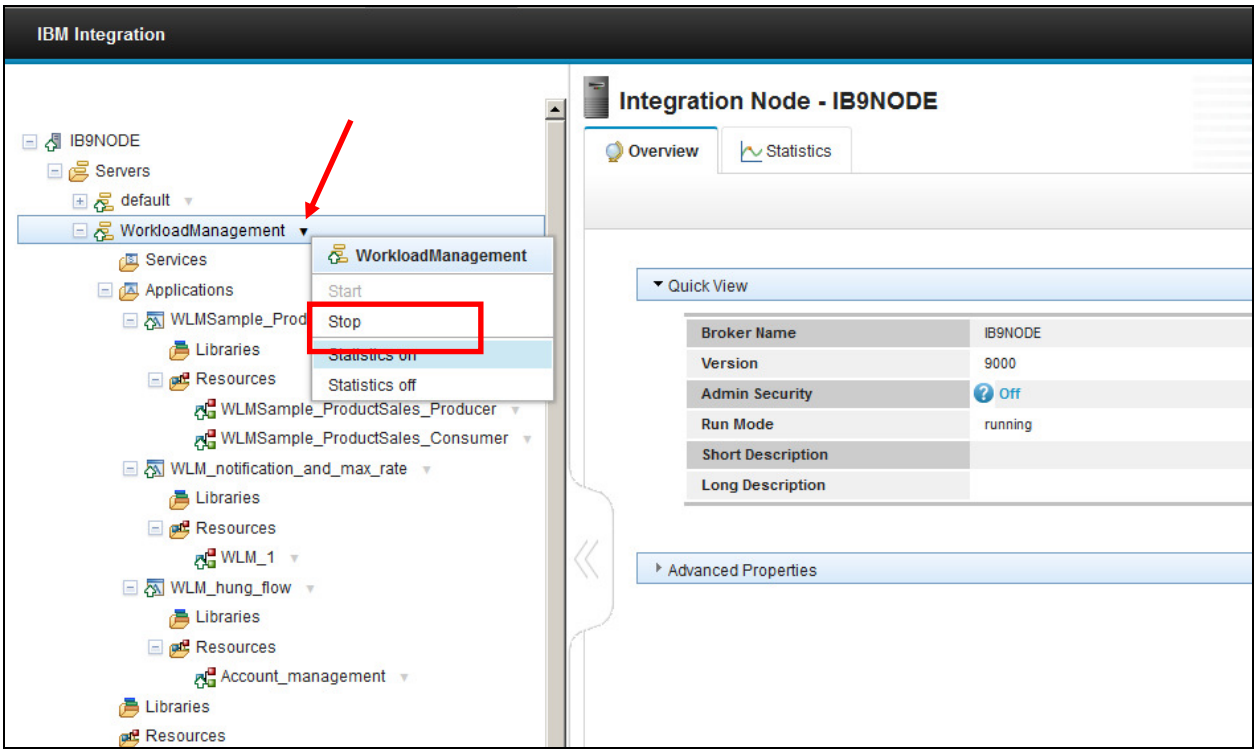


3. In the Servers section, expand Servers by clicking on the plus sign. Expand the WorkloadManagement server (execution group) and any deployed applications. You should see the applications you just deployed in the previous step.



4. You will see that you can Start and Stop the applications, as well as any defined server.

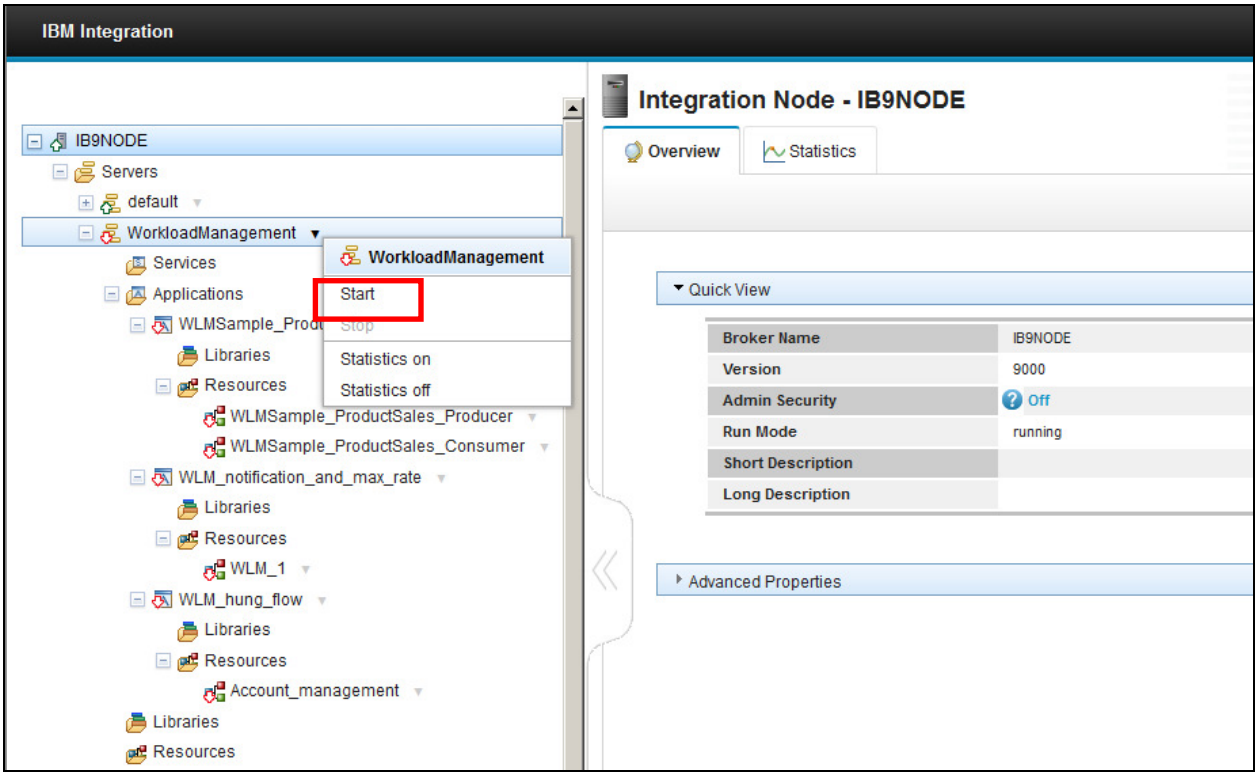
   Click on the WorkloadManagement server's context menu – down arrow beside the name - and select Stop.



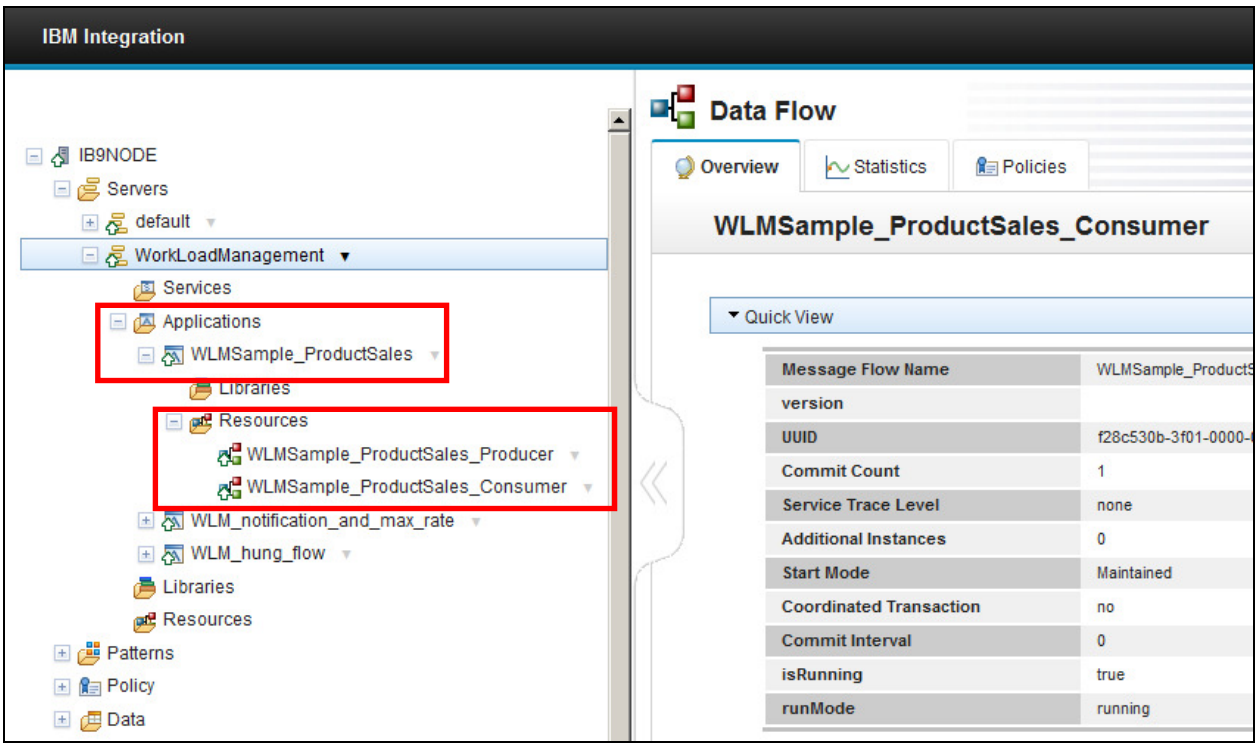
5. Wait for it to show stopped (red down arrow). Notice that all the Applications and Resources are stopped.

   Select the context menu again and select Start. The server will start and show a green “up arrow”.

   .



6. Try stopping and starting an application or message flow in the same manner.



4. Configure role-based security for web users

IBM Integration Bus provides the ability to control access to several broker functions through the web browser interface. This includes the ability to view and control the broker administration functions, as well as access to record/replay data, web pattern view and deployment, and policy settings. Different web users can have different access rights across these functions, and access can be granted, denied or revoked quickly.

Role-based security is achieved by using the existing security functions provided in Integration Bus and WebSphere MQ. Authorities are set on the appropriate queue in the underlying queue manager. For example, authorities for the Record/Replay function are defined by using the SYSTEM.BROKER.DC.AUTH queue.

The access authorities are defined against a set of user definitions which represent the available security roles. Each web user is then defined to use one or more of these security roles. For example, a Message Broker access definition might be made for a user called “RRView”. This user would have “view access” for the Record/Replay function, ie. it would have “inq” access for the SYSTEM.BROKER.DC.AUTH queue. The web user would then have a role access profile of “RRView”.

For the purposes of this lab, the pre-built system has several user roles. These have already been defined to the Windows operating system, and are represented by the following userids:

- ESBProfile1 (for Broker administration access, read-only)
- ESBProfile2 (for Broker administration access, update functions)
- ESBProfile3 (for Record/Replay users, not used in this lab)

Note that although these users are regular Windows accounts, they have been removed from the Windows login screen, in order to avoid inadvertently logging in to Windows with these users.

4.1 Activate security for IB9NODE

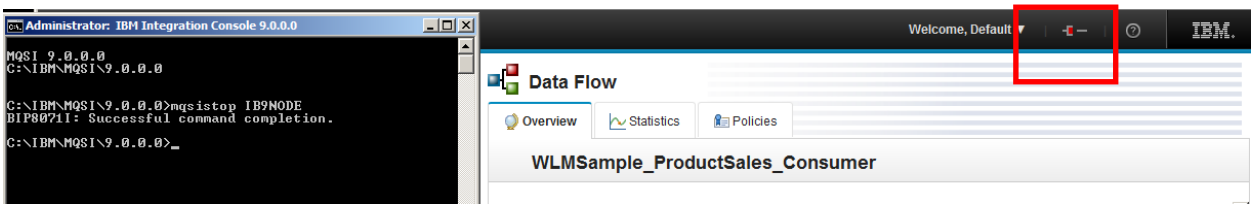
1. Open a Message Broker Command Console by double-clicking the desktop shortcut.

   Position the Firefox browser session with the Command Console window.

   Security can only be activated whilst the integration node is shutdown, so issue the following commands

   ```
   mqsistop IB9NODE
   ```

   When you issue the mqsistop, you will see the auto-refresh indicator turn red noting that the broker is not running. Hover over it and you will see a message indicating that “Real-time updates are disabled”.



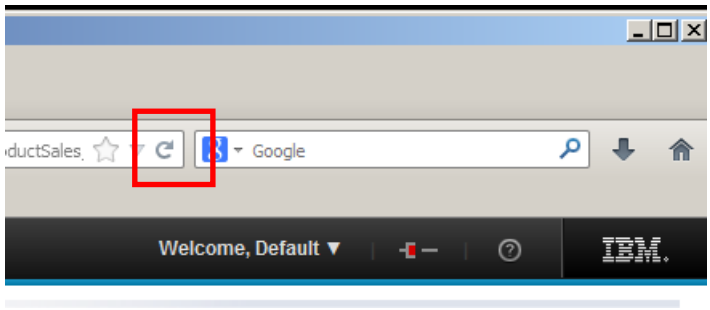
2. Set security on with the following command:

   ```
   mqsichangebroker IB9NODE -s active
   ```

   Restart the broker with the following command:

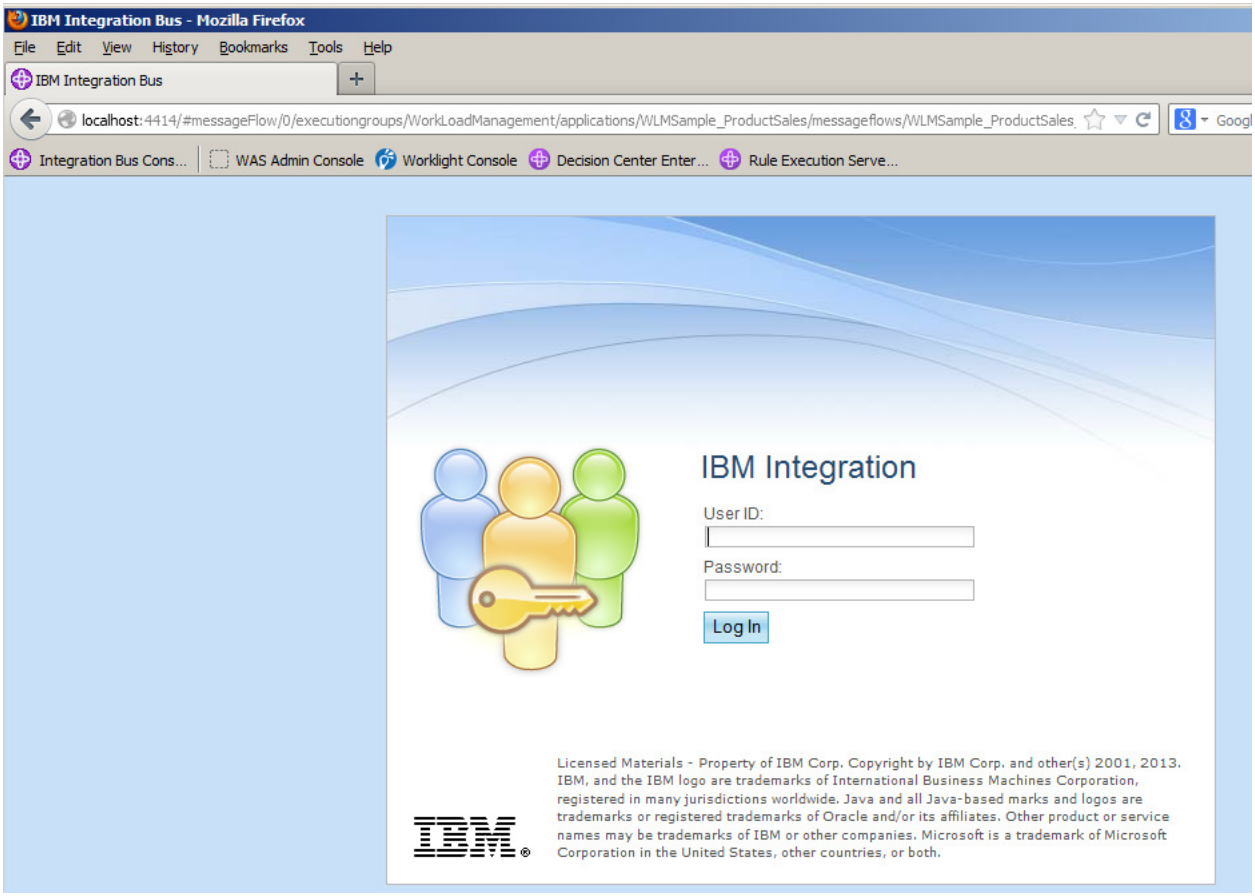
   ```
   mqsistart IB9NODE
   ```

3. After a short while, reload the browser page by clicking the indicator in the address page.



4. You are now presented with a sign-on screen since security has been activated.

   Before you can continue, we must configure security so you are able to sign in, so continue with the next step.



4.2 Define the MQ authorities for the web users

1. Security for the Web Admin user interface is managed using MQ authorities. These MQ authorities are specified for the system usernames mentioned above (eg. ESBProfile1), which are then referenced by the Integration Bus web user definitions.

   The following table shows the MQ authorities that are required for different types of users:

   1) Web admin users (required for all users)

MQ Object	MQ Authority
Queue Manager	Connect, Inquire
SYSTEM.DEPLOY.QUEUE	Put
SYSTEM.DEPLOY.REPLY	Get, Put
SYSTEM.BROKER.AUTH	Inq
SYSTEM.BROKER.AUTH.execgroup	Inq

   2) Web admin users (additional for update functions, eg. stop/start message flow)

MQ Object	MQ Authority
SYSTEM.BROKER.AUTH	Inq, Put, Set
SYSTEM.BROKER.AUTH.execgroup	Inq, Put, Set

   You will define the MQ Authorities for the following principals:

   ```
   ESBProfile1 - web admin user, readonly
   ESBProfile2 - web admin user, update (start/stop)
   ```

   These definitions can be made through the IB Explorer (see the following paragraphs). However, the commands have been provided for you in a command file. In the command console, change directory to c:\student \ webadmin \ resources.

   Run the command:

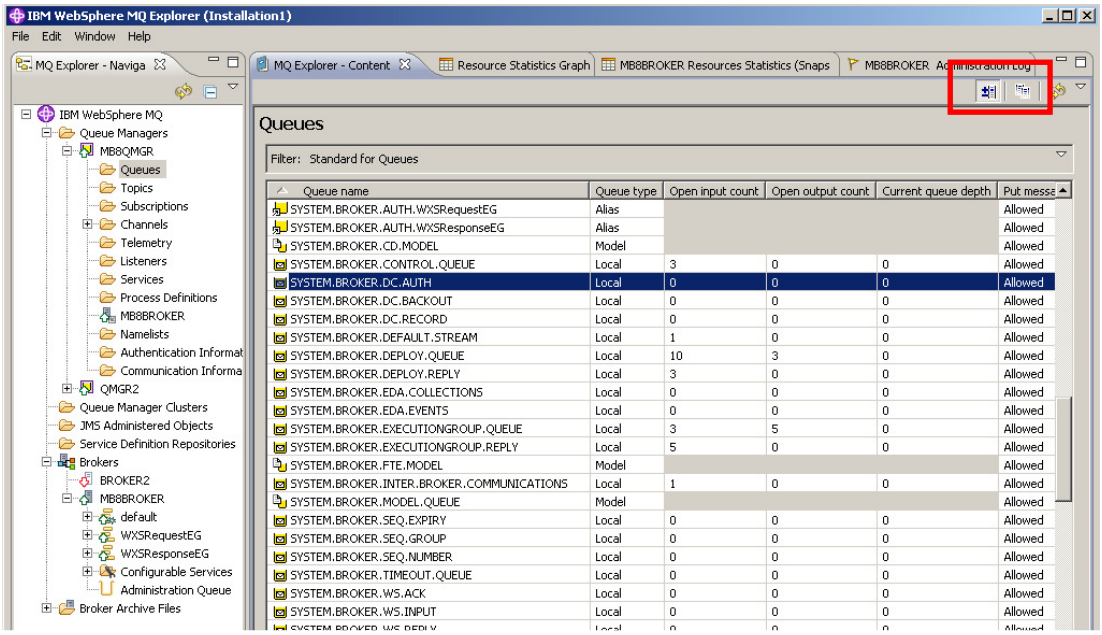
   `Set_webadmin_users_MQAuth.cmd`

   This will run several “setmqaut” commands to create the required authorities. You can examine these in more detail by editing the above command file.

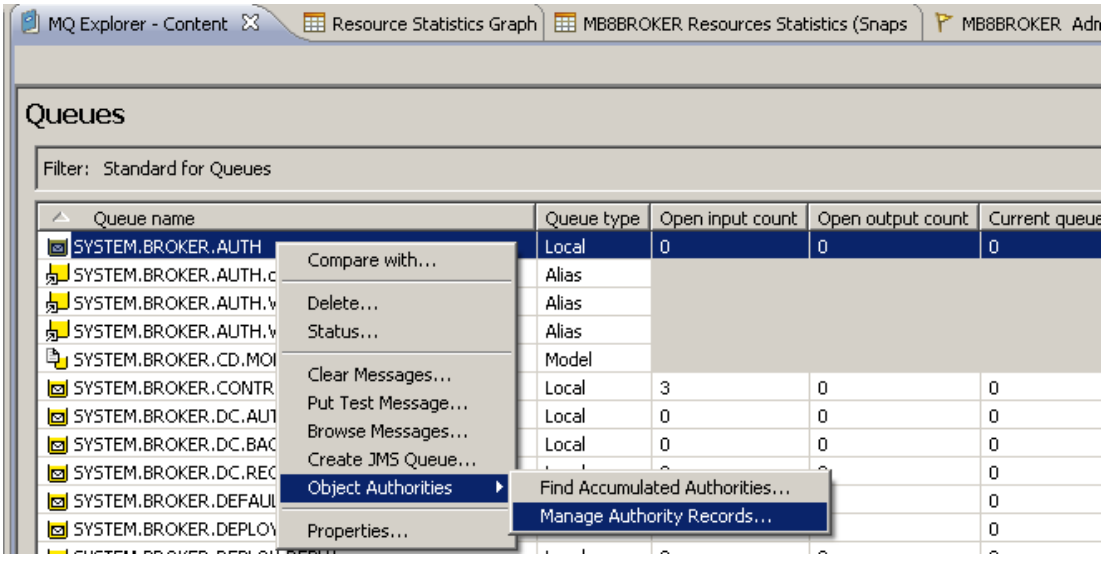
4.3 Define the MQ authorities manually (optional)

1. If you want to make the security definitions manually, in the MQ Explorer, expand the IB9QMGR queue manager, and select Queues. Ensure the Systems queues are displayed (you may need to click the “Show System Objects” button).

   Otherwise, skip straight to the next section, define the Web Users.

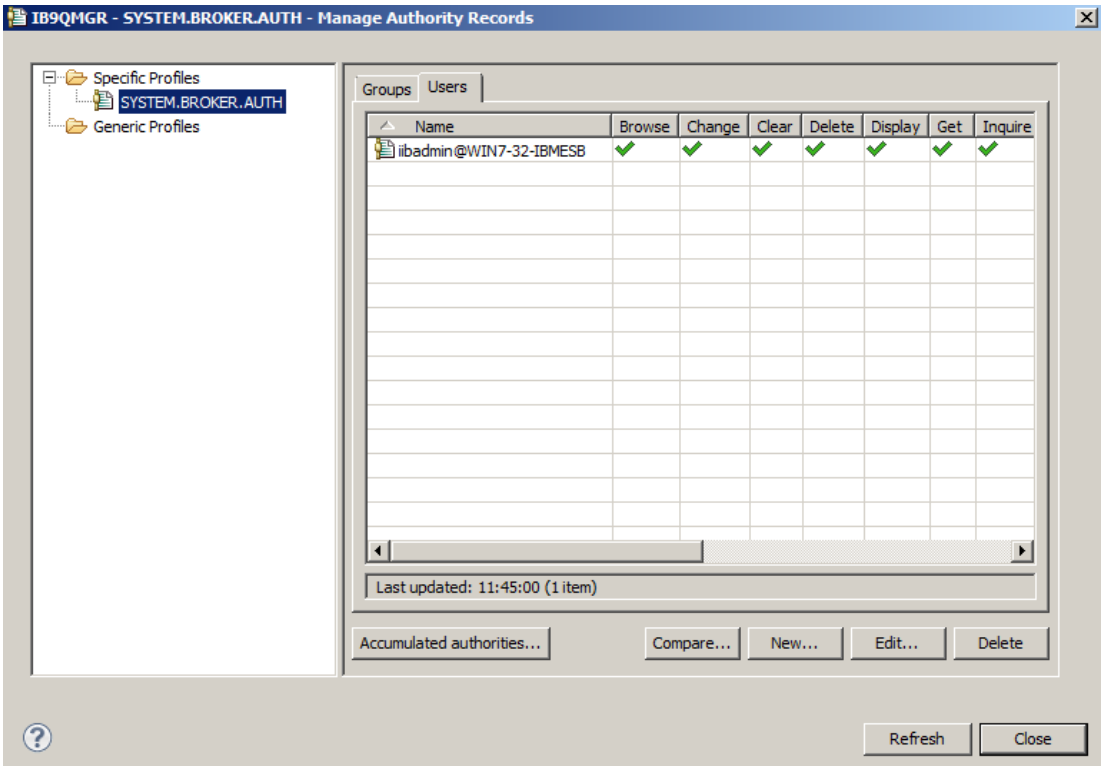


2. Right-click the SYSTEM.BROKER.AUTH queue, and select Object Authorities, Manage Authority Records.



3. Expand “Specific Profiles”, and click SYSTEM.BROKER.AUTH.

   Select the Users tab.

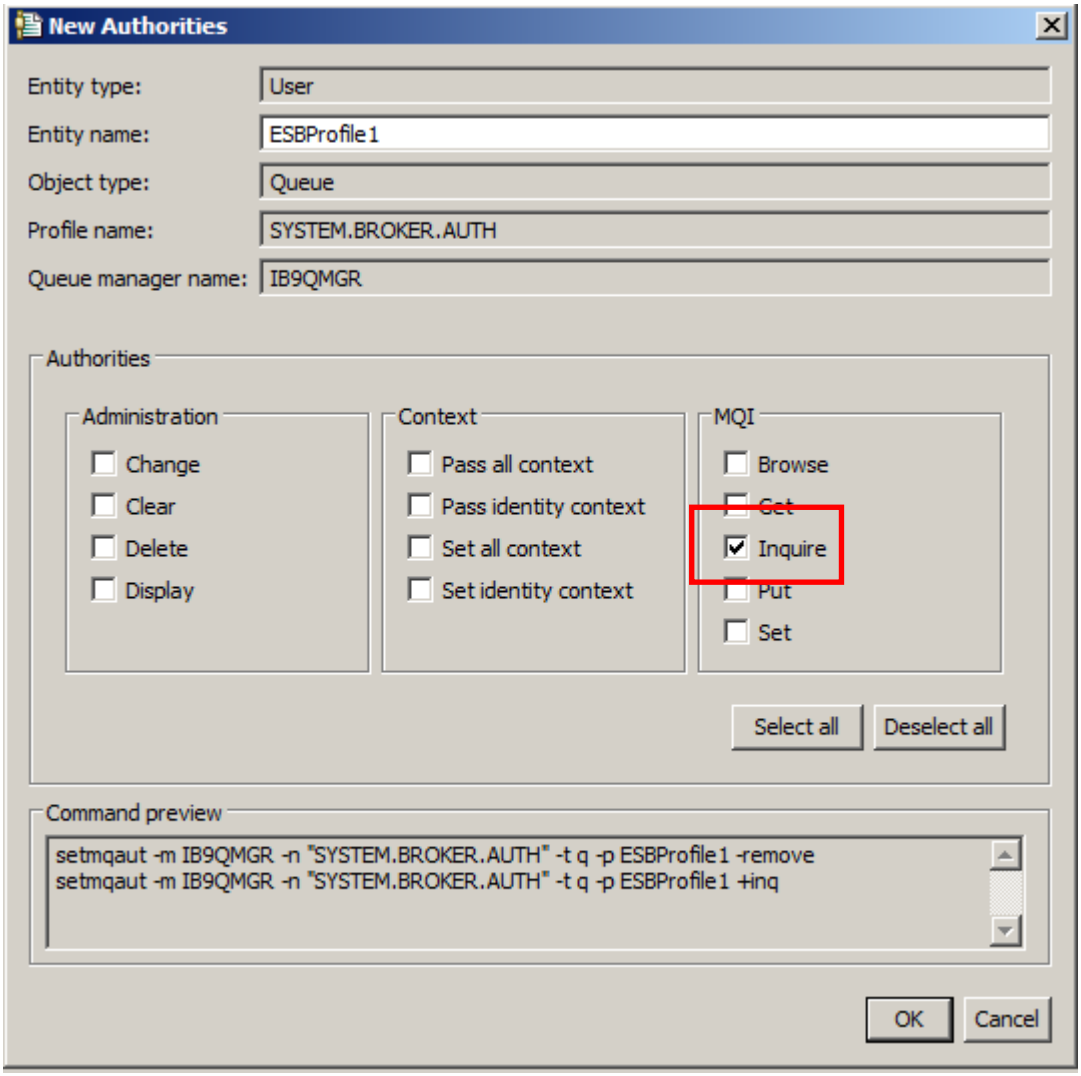


4. Ensure Users are selected, and click New.

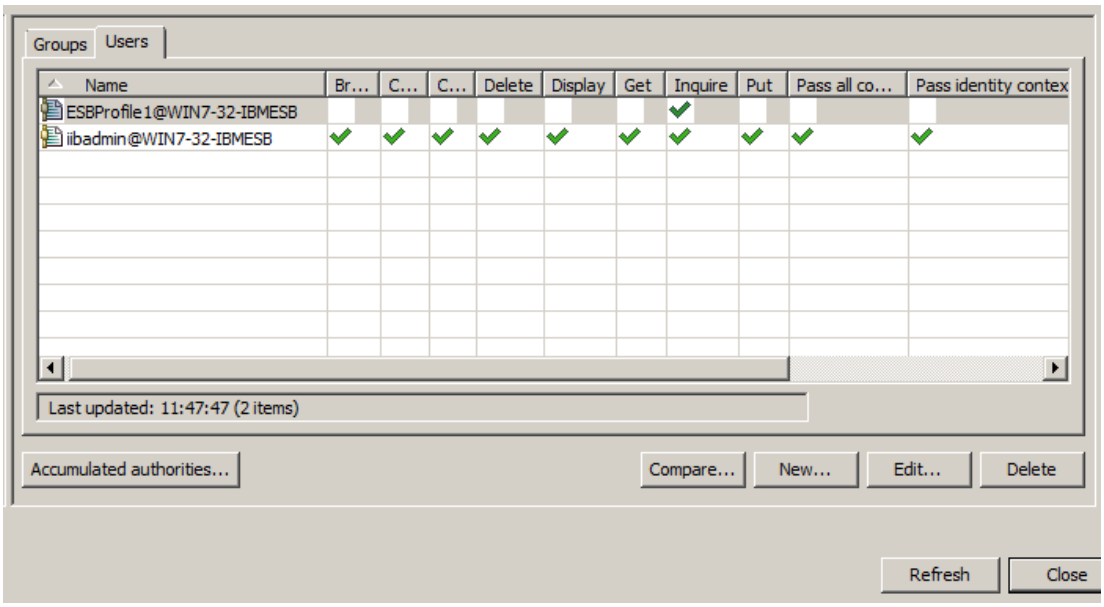
   Set Entity name = ESBProfile1

   Set Inquire = ticked

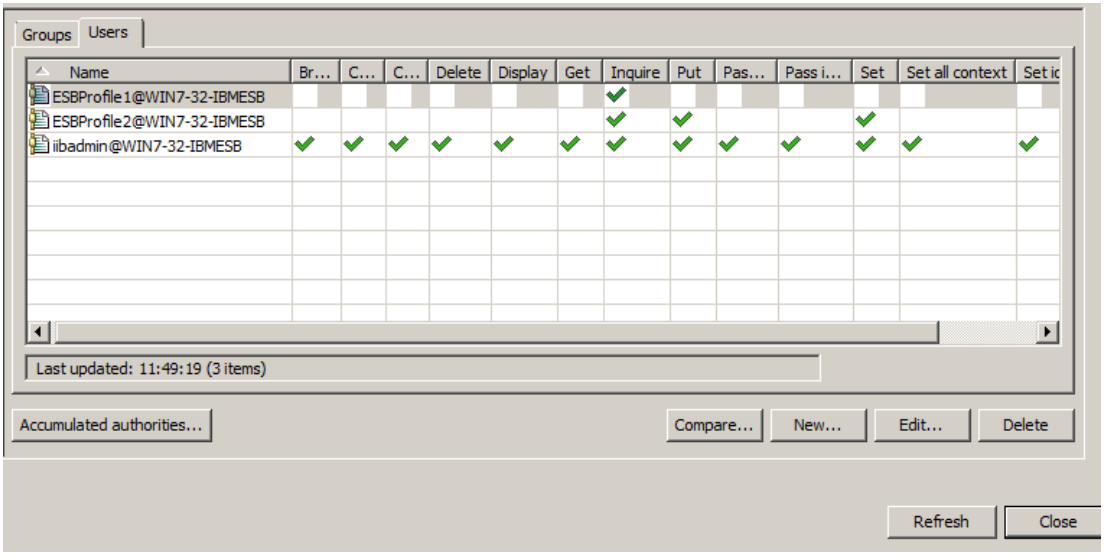
   Click OK.



5. The new user will be added. Note that this user will just have Inquire authority.



6. Add another user, ESBProfile2. This user should have Inq, Put and Set authorities.



7. Note – the above optional section shows only a subset of the required permissions. If you wish to complete this task manually (using the MQ Explorer), you should ensure that the following MQ authorities are created. If you ran the script to create the MQ authorities, these will have been created for you.

ESBProfile1

Queue manager	
IB9QMGR	+connect +inq
Queues:	
SYSTEM.BROKER.AUTH	+inq
SYSTEM.BROKER.AUTH.default	+inq
SYSTEM.BROKER.AUTH.WorkloadManagement	+inq
SYSTEM.BROKER.DEPLOY.QUEUE	+put
SYSTEM.BROKER.DEPLOY.REPLY	+get +put
SYSTEM.BROKER.WEBADMIN.SUBSCRIPTION	+get +put
Topic	
SYSTEM.BROKER.MB.TOPIC	+pub +sub

ESBProfile2

Queue manager	
IB9QMGR	+connect +inq
Queues:	
SYSTEM.BROKER.AUTH	+inq +put +set
SYSTEM.BROKER.AUTH.default	+inq +put +set
SYSTEM.BROKER.AUTH.WorkloadManagement	+inq +put +set
SYSTEM.BROKER.DEPLOY.QUEUE	+put
SYSTEM.BROKER.DEPLOY.REPLY	+get +put
SYSTEM.BROKER.WEBADMIN.SUBSCRIPTION	+get +put
Topic	
SYSTEM.BROKER.MB.TOPIC	+pub +sub

4.4 Define the web users for IB9NODE

1. Define an Integration Bus web user for read-only access. This user will be able to see what applications are deployed, but will not be able to control the status of these applications.

   In an Integration Bus Command Console, run the command

   ```
   mqsiwebuseradmin IB9NODE
         -c
         -u admin1
         -a passw0rd
         -r ESBProfile1
   ```

   This command will define a new web user, admin1. The user will have the security profile defined by the associated role, which in this case will mean that the user can only view the broker and any deployed applications.

2. Define a Message Broker web user for update access. This user will be able to see what applications are deployed, and will be able to control the status of these applications (start/stop, etc).

   In a Message Broker Command Console, run the command

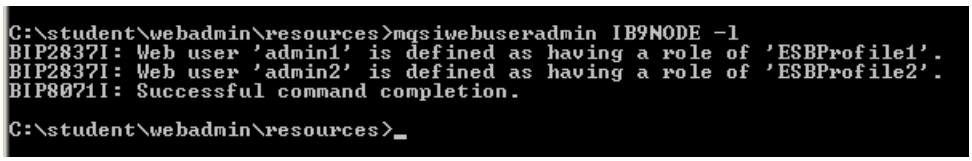
   ```
   mqsiwebuseradmin IB9NODE
         -c
         -u admin2
         -a passw0rd
         -r ESBProfile2
   ```

   This command will define a new web user, admin2. The user will have the security profile defined by the associated role, which in this case will mean that the user will be able to view the broker and execution groups, and any deployed applications, as well as control their status.

3. Display the newly-defined web users by running the command

   ```
   mqsiwebuseradmin IB9NODE -l
   ```

   ```
   C:\student\RecordReplay\webadmin>mqsiwebuseradmin IB9NODE -l
   BIP2837I: Web user 'admin1' is defined as having a role of 'ESBProfile1'.
   BIP2837I: Web user 'admin2' is defined as having a role of 'ESBProfile2'.
   BIP8071I: Successful command completion.
   ```

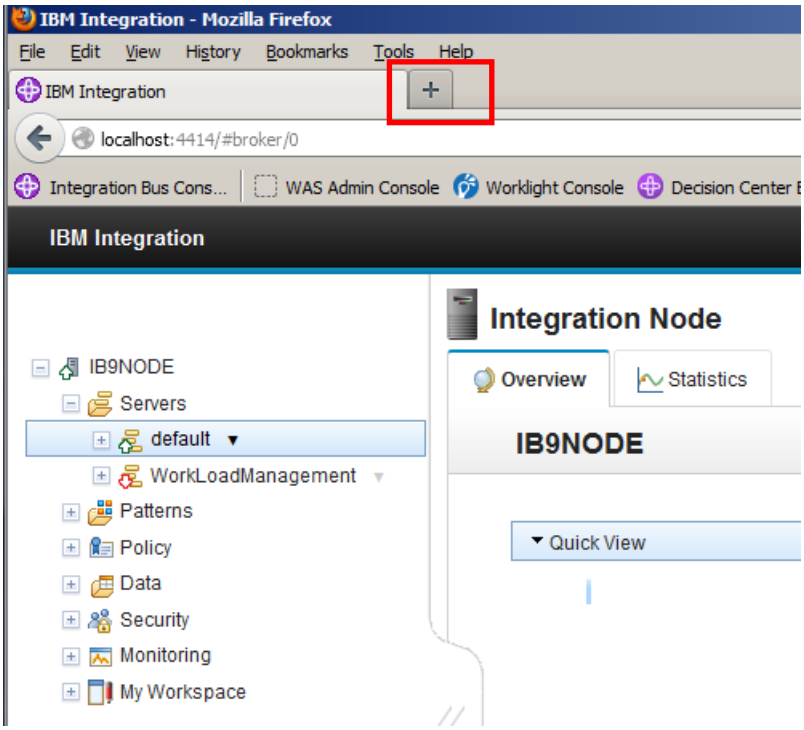


5. Using the Web Admin interface with security

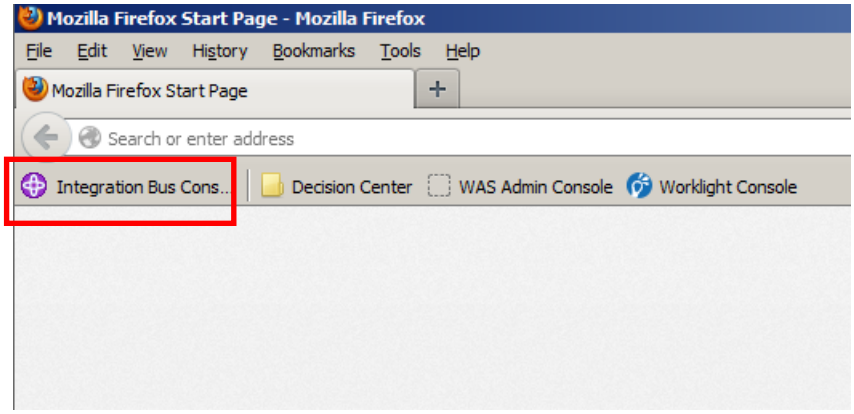
5.1 The web admin interface for a read-only user

Now that security has been configured for Web Admin users, we will login as the admin1 user, which is read-only, and see what the browser interface offers for someone who can only view the Integration Node.

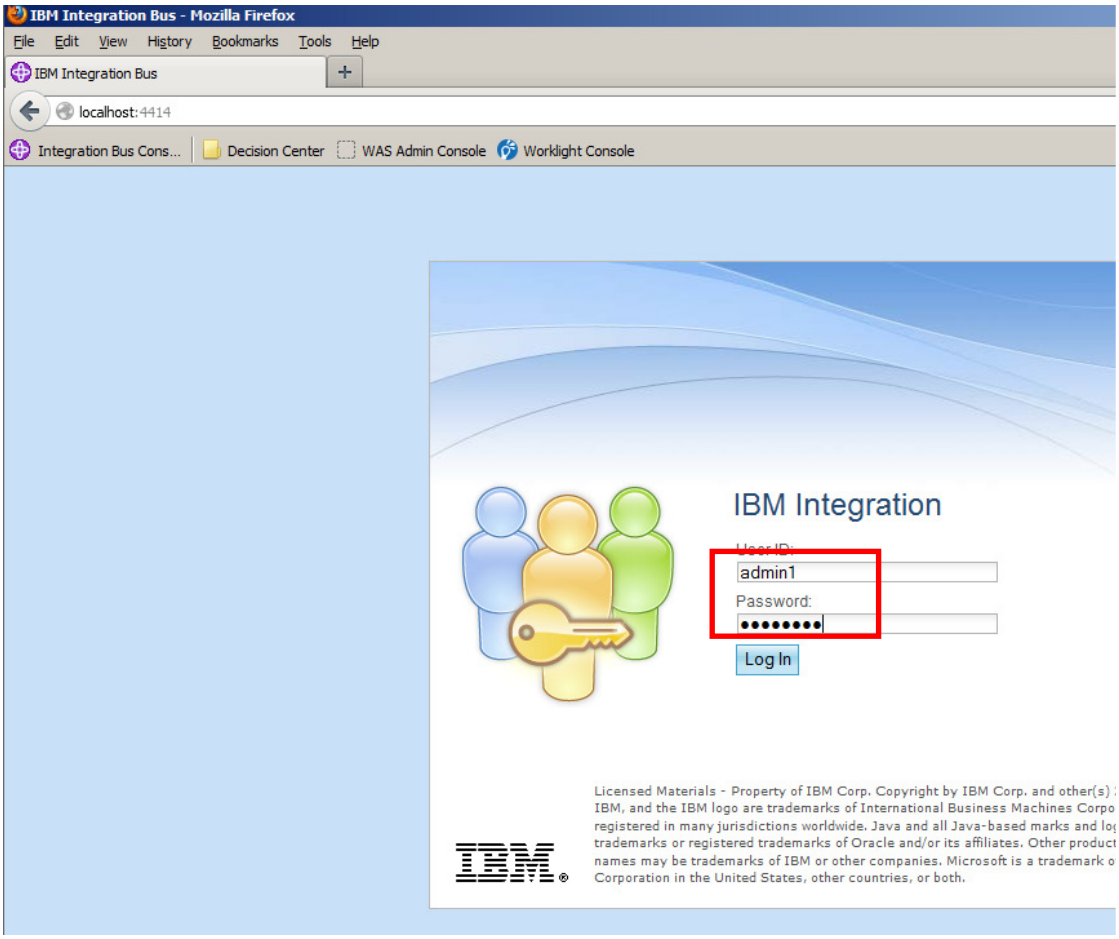
1. Open a new Firefox web browser by clicking the plus (+) next to IBM Integration at the top of the browser window (above the URL). You should still have an open browser if you did not close it previously. You may use that one or open a new one.



2. Click the provided shortcut link, http://localhost:4414.

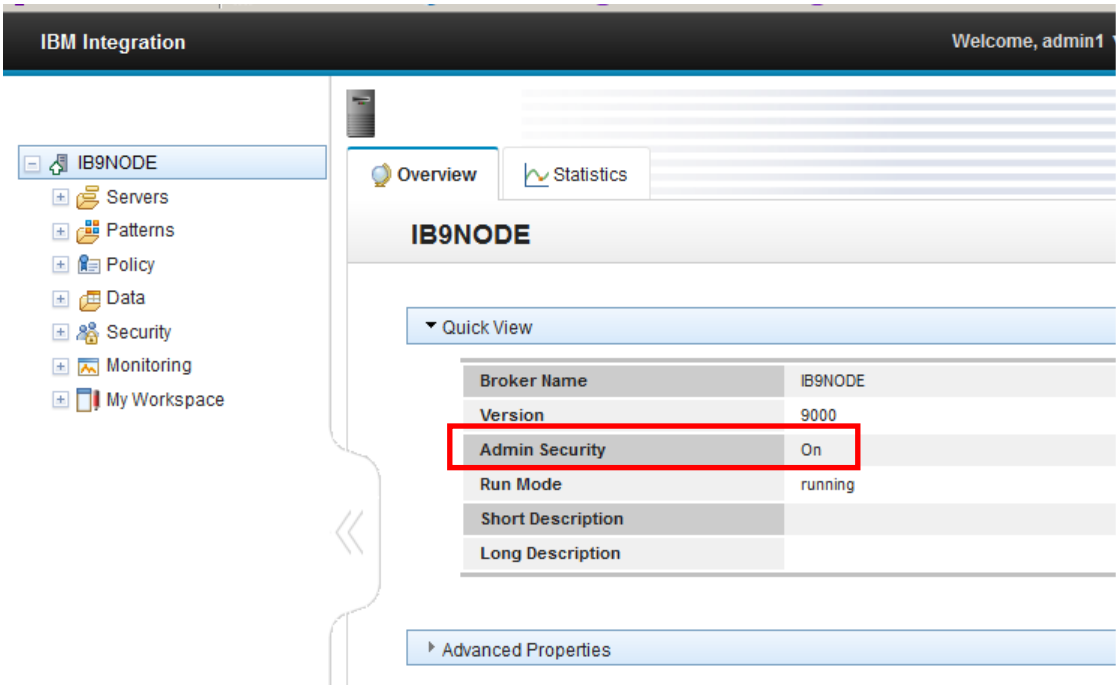


This time, you will be presented with a login screen. Login with the userid admin1 (password is passw0rd).



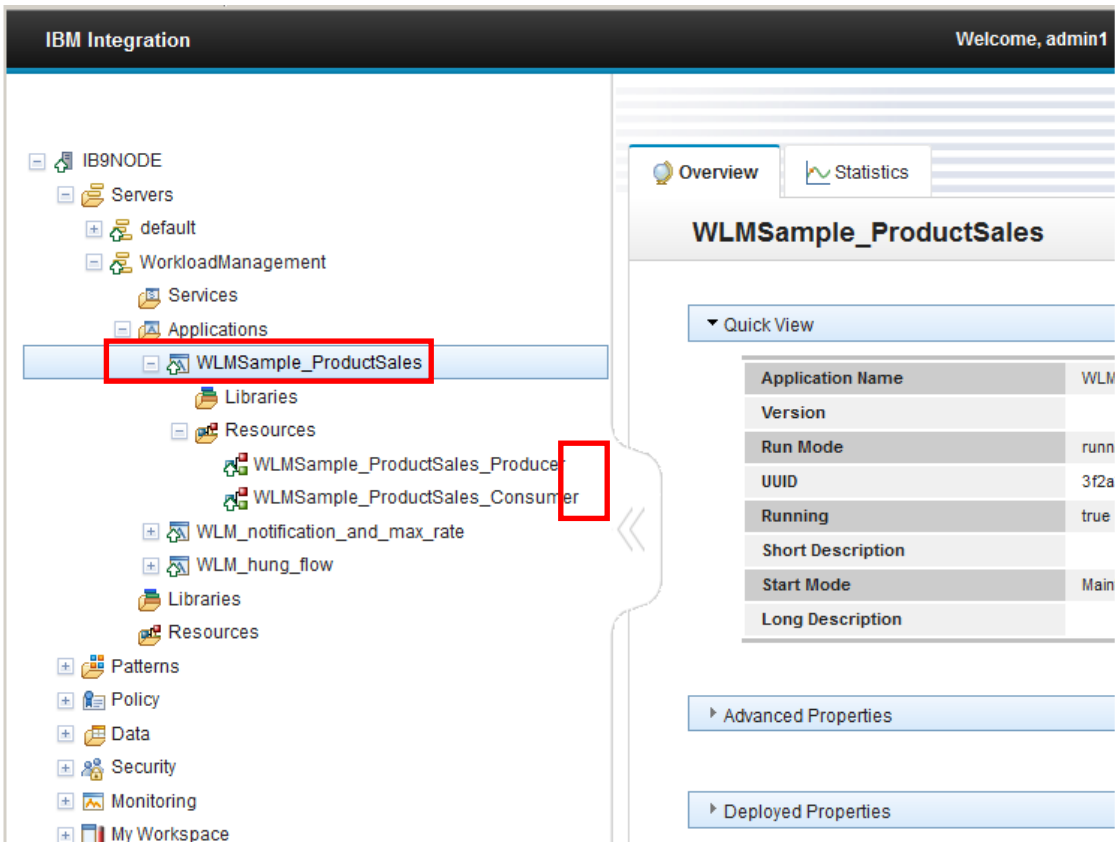
3. This user has read-only access to the node.

   Note that the Quick View will now show you that Admin Security is active.



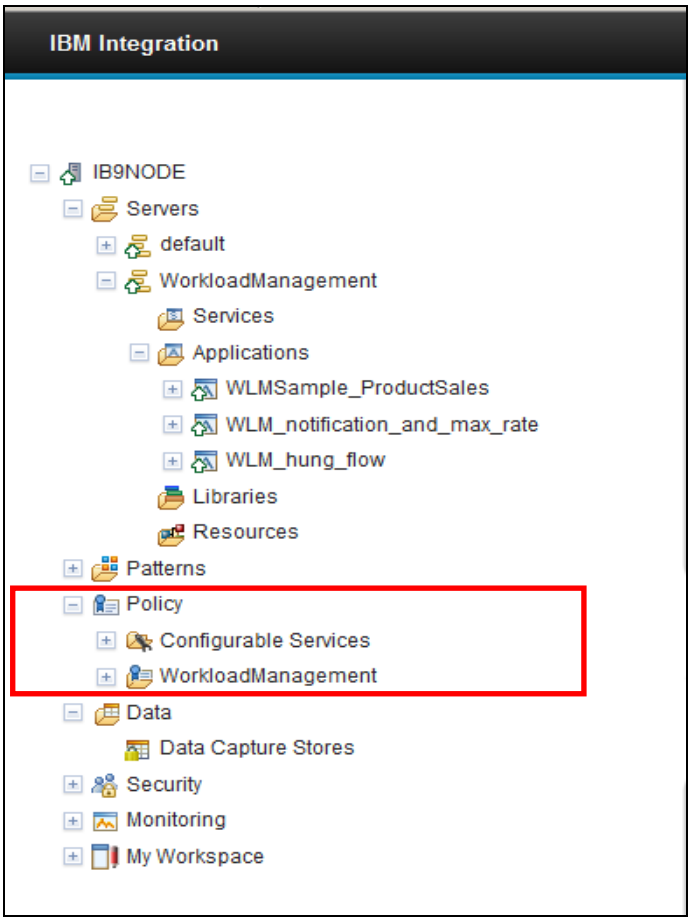
4. Expand the Servers category, and expand any deployed applications and services. The screen below shows several deployed applications.

   Note that clicking on any of the deployed applications in the navigator will show the details of the application. However, this user will not be able to start or stop the deployed applications, since the security profile is “read only”. You will not see any pull-down context menus as you did previously.



5. Notice that although you are able to expand the policy folder and study existing policies you do not have permission to edit, create or delete policies.

   Expand the Data category (this is used for the Record/Replay data). You will see the Data Capture Stores heading, but no capture stores will be visible. This is because this user does not have access to any Record/Replay facilities (see the Record/Replay or Trades lab).

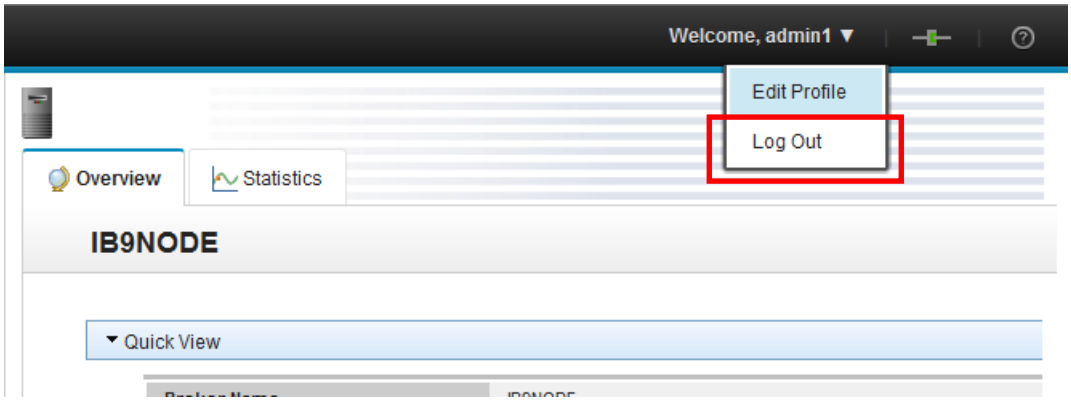


5.2 The Web Admin interface for a user with update access

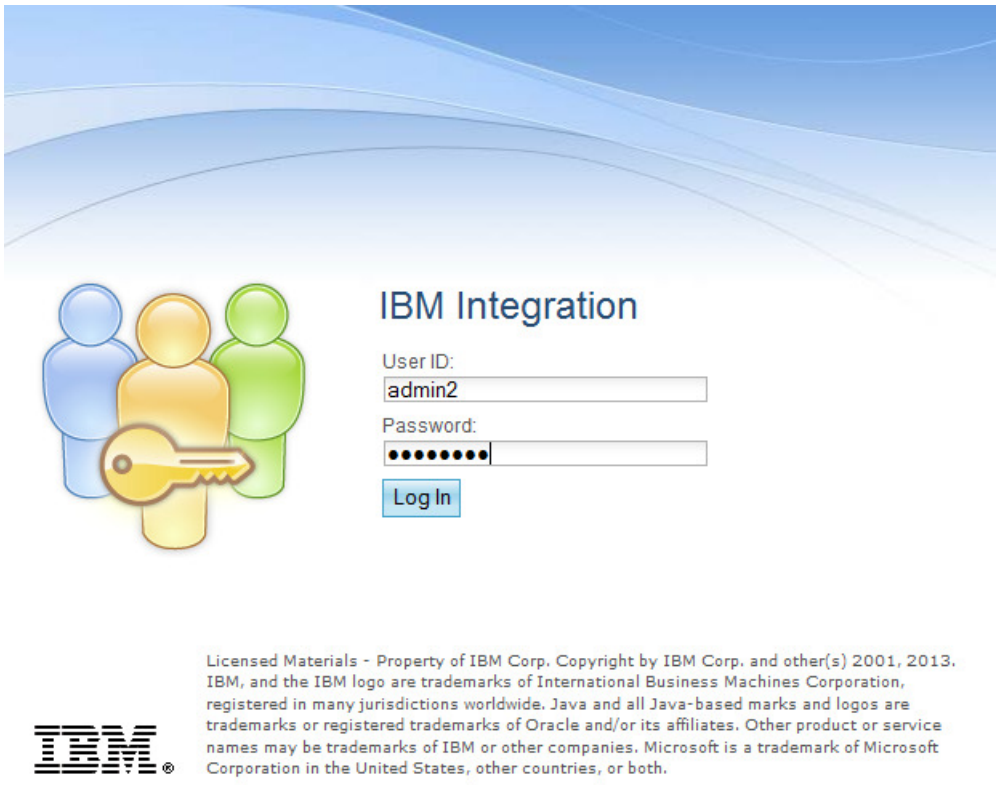
Now that security has been configured for Web Admin users, we will login as the admin2 user which is the update user. This user has full functionality for stopping and starting resources and for creating and deleting policies.

1. After exploring the facilities for admin1, logout admin1.

   Click the pull-down beside the Welcome, admin1 banner and select Log Out.

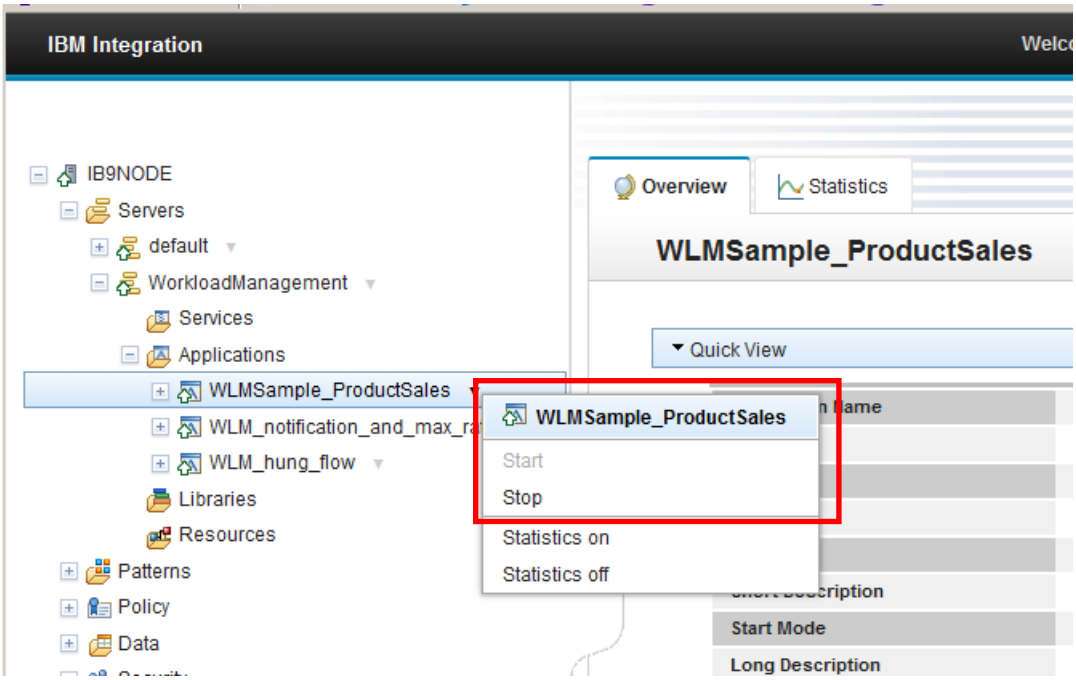


   Log-in as admin2 (password is passw0rd).



2. As before, expand the deployed applications. You will see that this user has the ability to Start and Stop the deployed applications, by clicking on the arrow on the right of the item in the navigator.

   Click on the WLMSample_ProductSales application. Then click on the pull-down to the right of the application and select **Stop**.

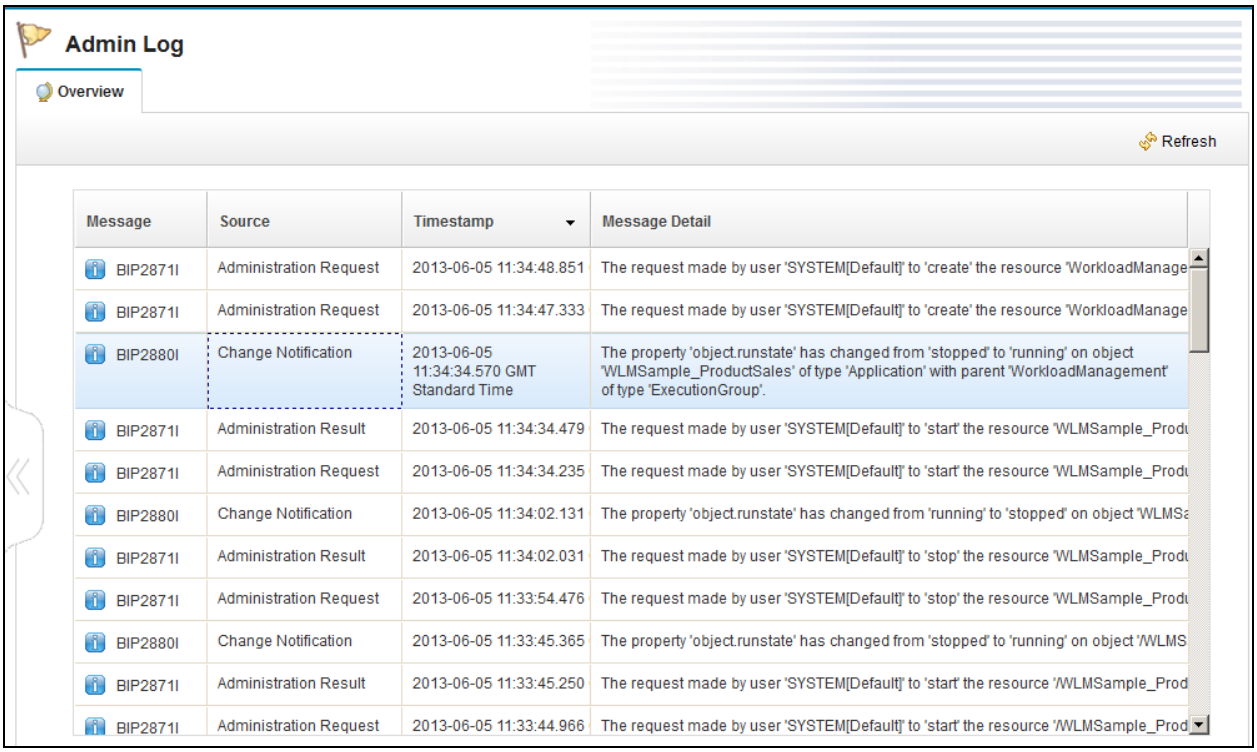


   The application will stop.

   Restart the WLM_ProductSales application.

3. Expand the Monitoring item, and click Admin Log. All broker log messages will be displayed. The most recent Change Notification item will be the restart of the application.

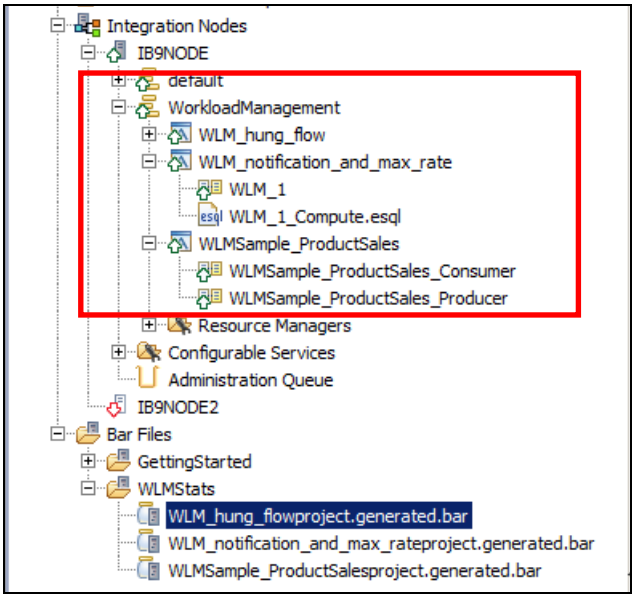
   To see the message detail of the message, hover over the latest Change Notification under the Source column. It will change to a hot link. Click on it and the message will be expanded to show the full text.



6. Exploring the Web Admin flow statistics facilities

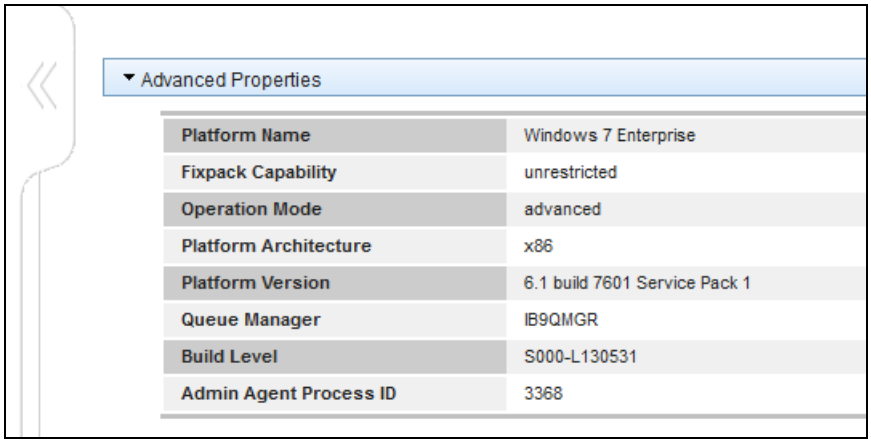
6.1 Investigate the statistics function in the web admin interface

1. Earlier in the lab, you deployed the barfiles for the applications we will use to generate statistics. Check the IB Explorer to make sure the applications and message flows are running in the WorkloadManagement integration server.

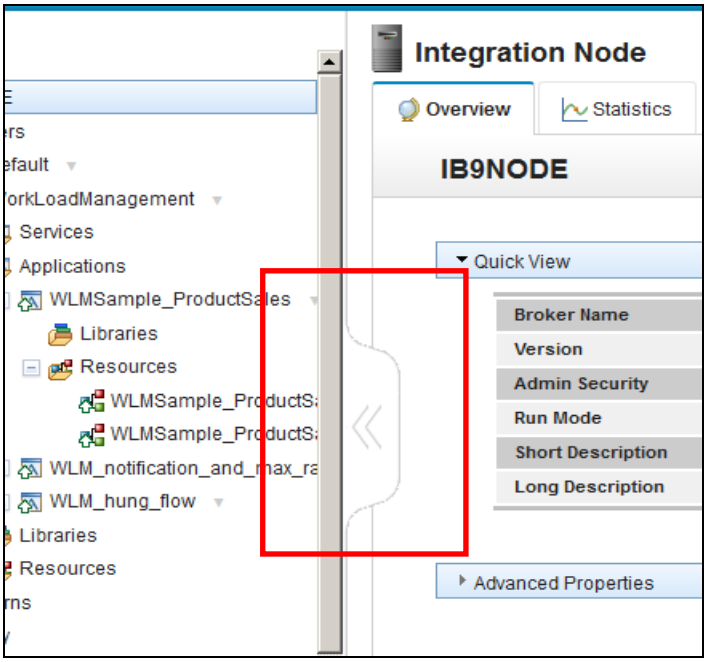


2. Return to the Web Browser admin tool, and click the IB9NODE node.

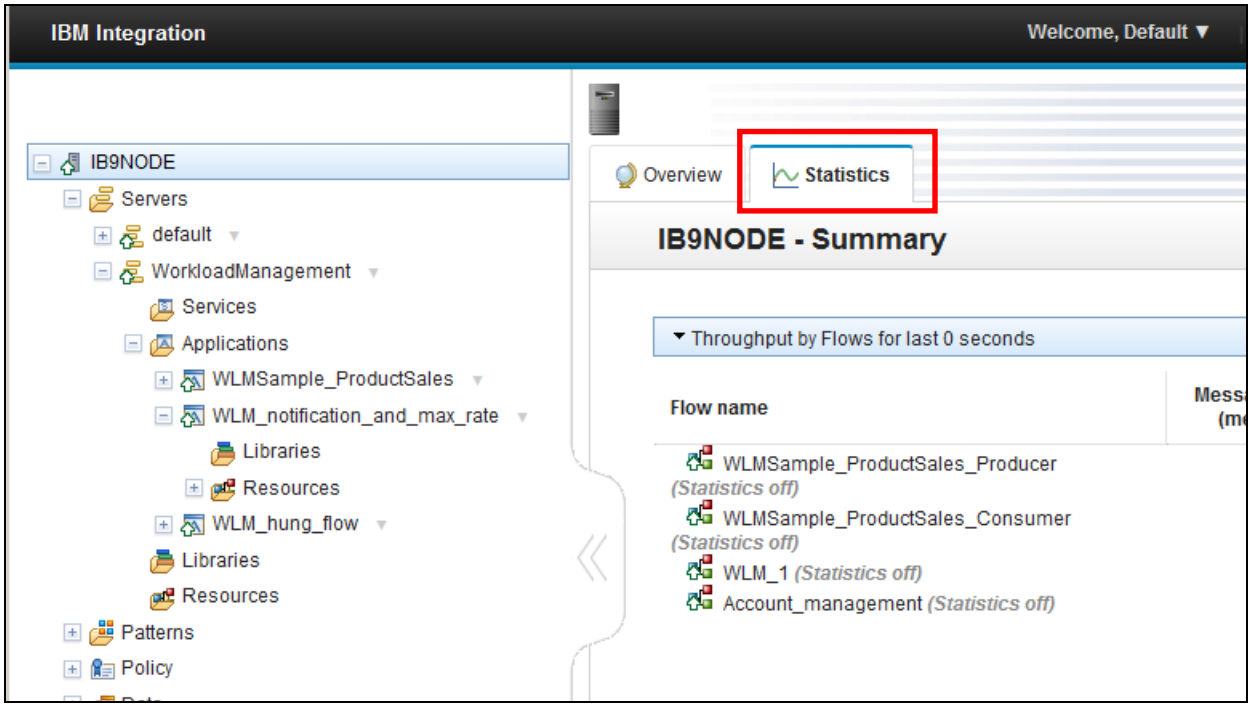
   We looked at the Quick View earlier when discussing security. Scroll down to see the Advanced Properties where you will find information about the platform which the node is running on as well as the queue manager name supporting the node.



3. As before, expand the servers and deployed applications. As you expand the sub-folders, the navigator (vertical sliding bar) should automatically adjust, but you may need to adjust the viewable area by grabbing and sliding the navigator to your liking.

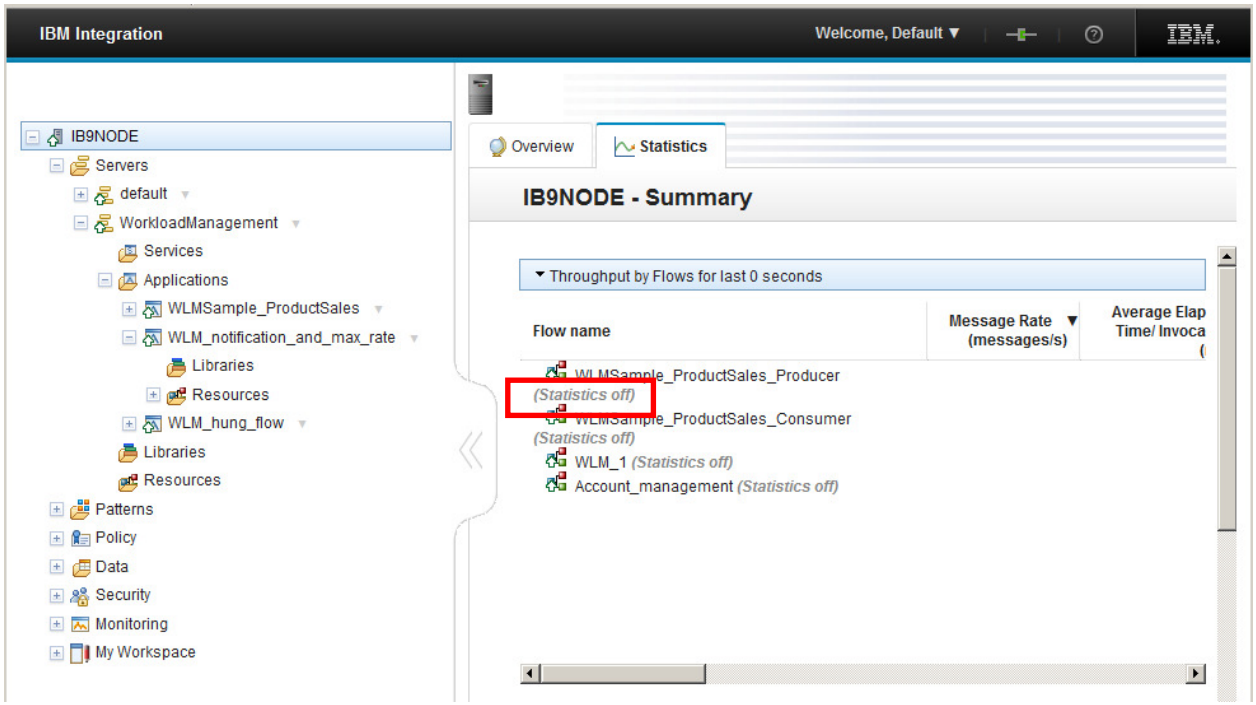


4. Click on the Statistics tab.



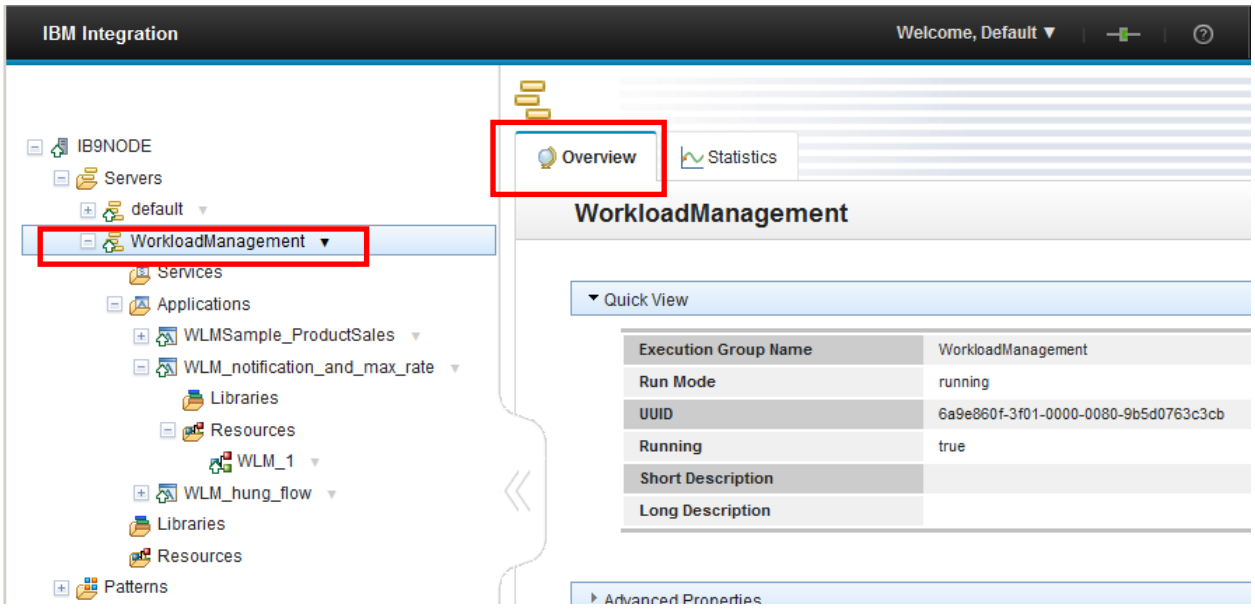
You will see the flows that are deployed to all integration servers. You should not see any flow statistics yet because we have not sent any data to the flows to be processed. Also, we have not yet turned statistics on for any of the flows.

5. If not fully expanded, expand the two categories – “Throughput by Flows for last seconds” and “Nodes for all flows in IB9NODE”.

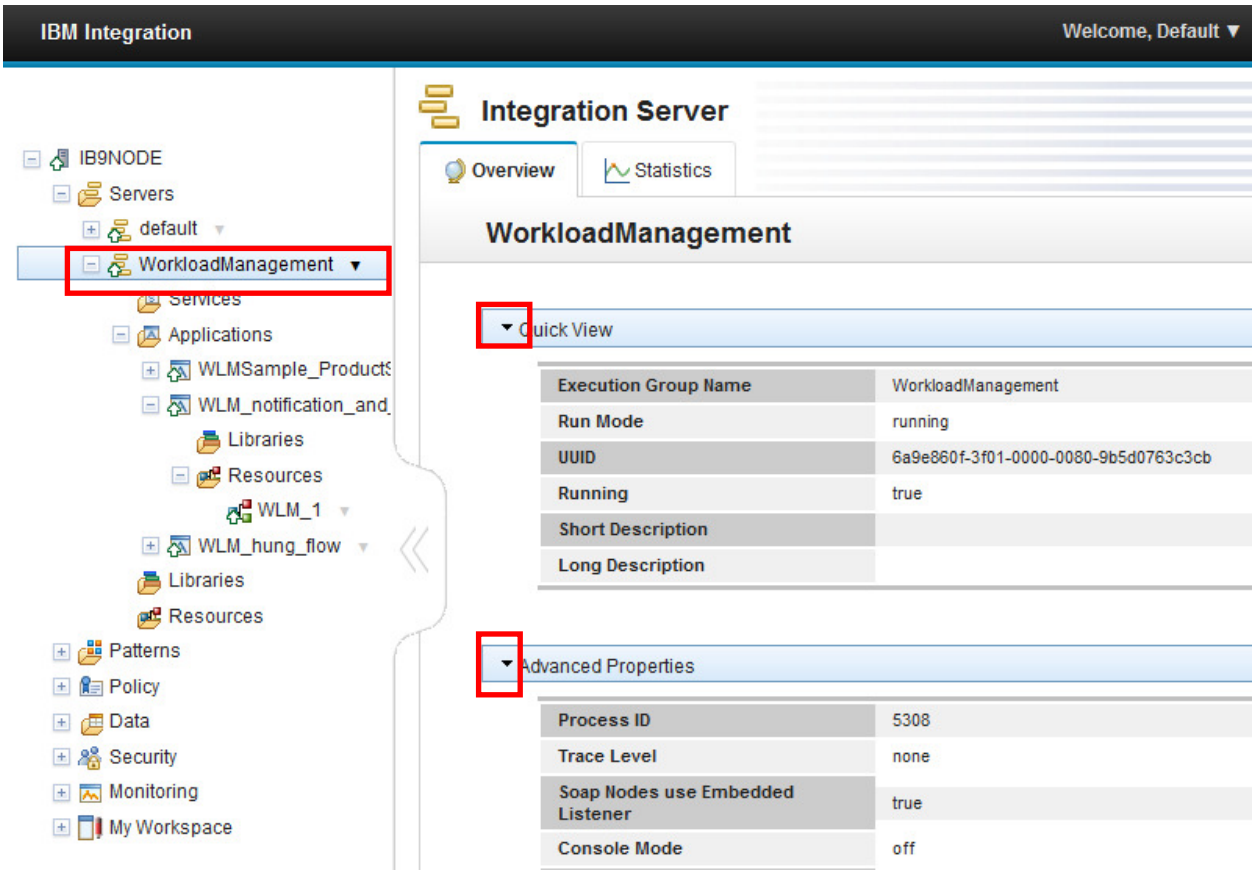


You can see that statistics are off for the flows. Scroll to the right or adjust the navigator to observe the columns indicating statistics which statistics will be captured.

6. Click on the WorkloadManagement server. You are taken to the Overview panel for the WorkloadManagement integration server.



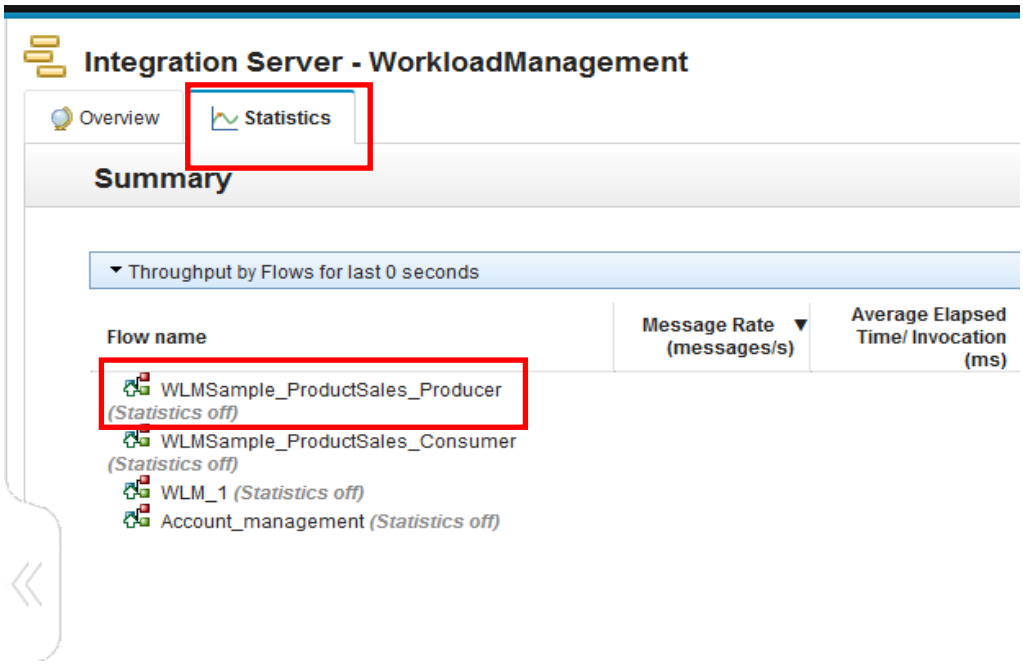
7. The Quick View is expanded for you. You may collapse it if you are not interested in the general information. Expand Advanced Properties also.



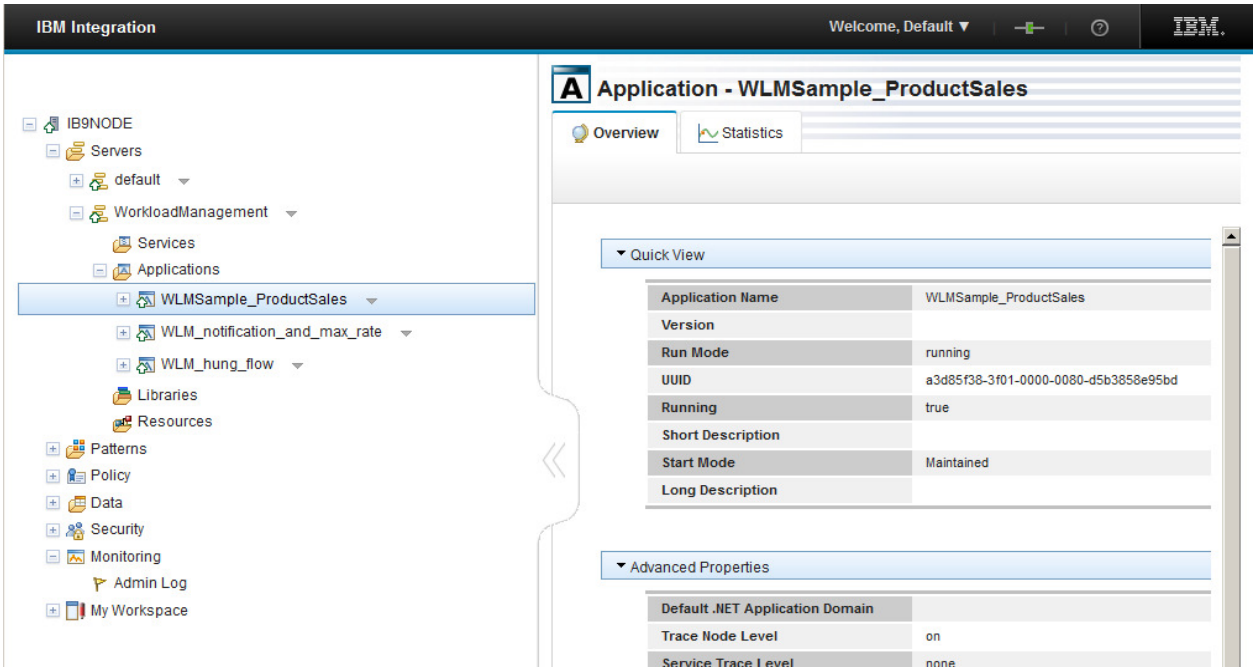
The Quick View panel displays important information about the execution group such as its name, UUID, Run Mode. If necessary, scroll down to see the Advanced Properties.

Advanced Properties show more detailed information such as Process ID, Trace Level, and exits. Review the Quick View and Advanced Properties.

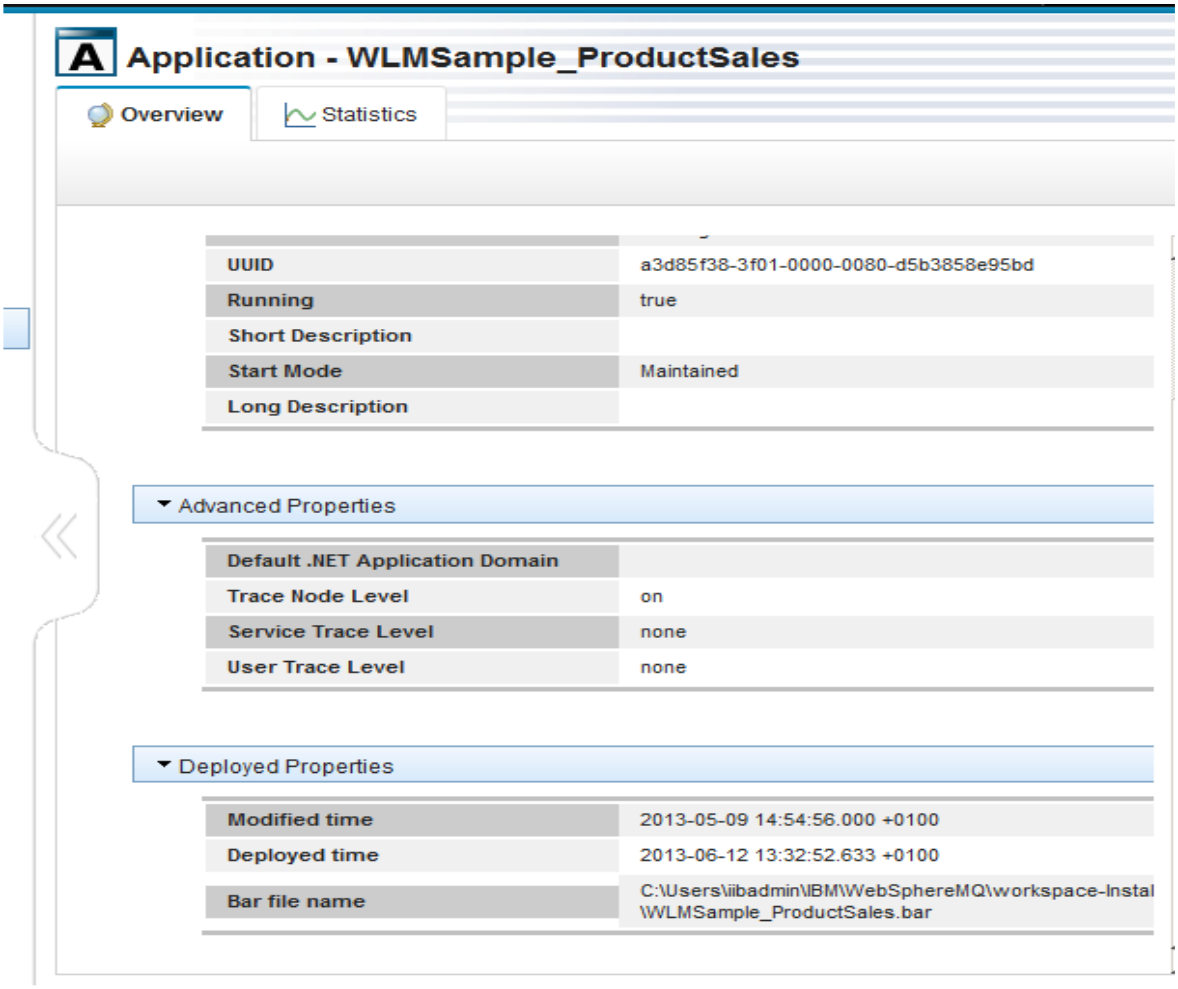
8. Click Statistics. Expand the groups if they are collapsed. At the Server level, you will only see the flows running in that particular server. Again, note that Statistics are currently off for the flows.



9. Expand Applications and click WLMSample_ProductSales. Again you see a Quick View which gives you the application name, UUID, and status.

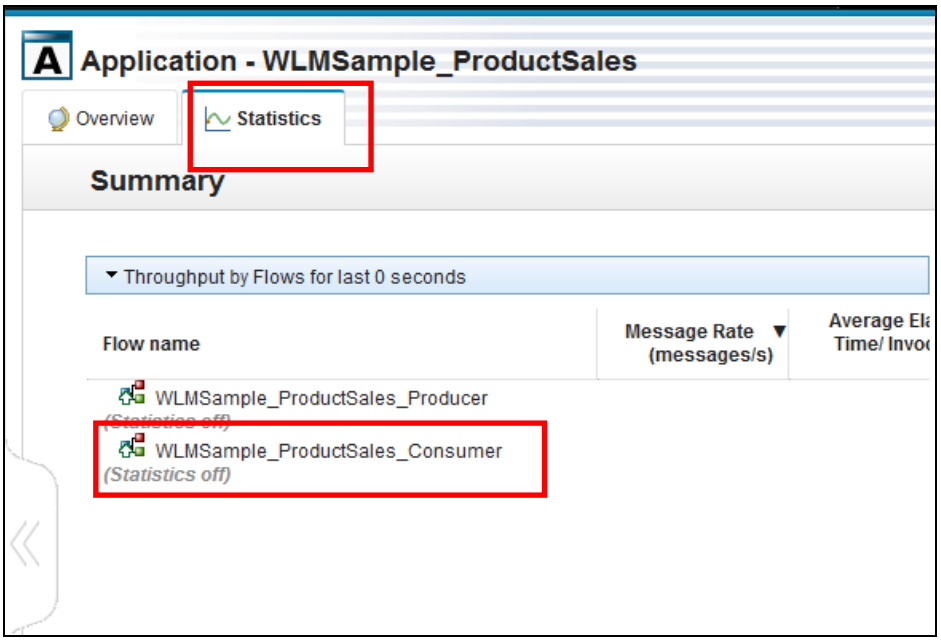


10. Expand Advanced Properties and Deployed Properties. Review the information found here.

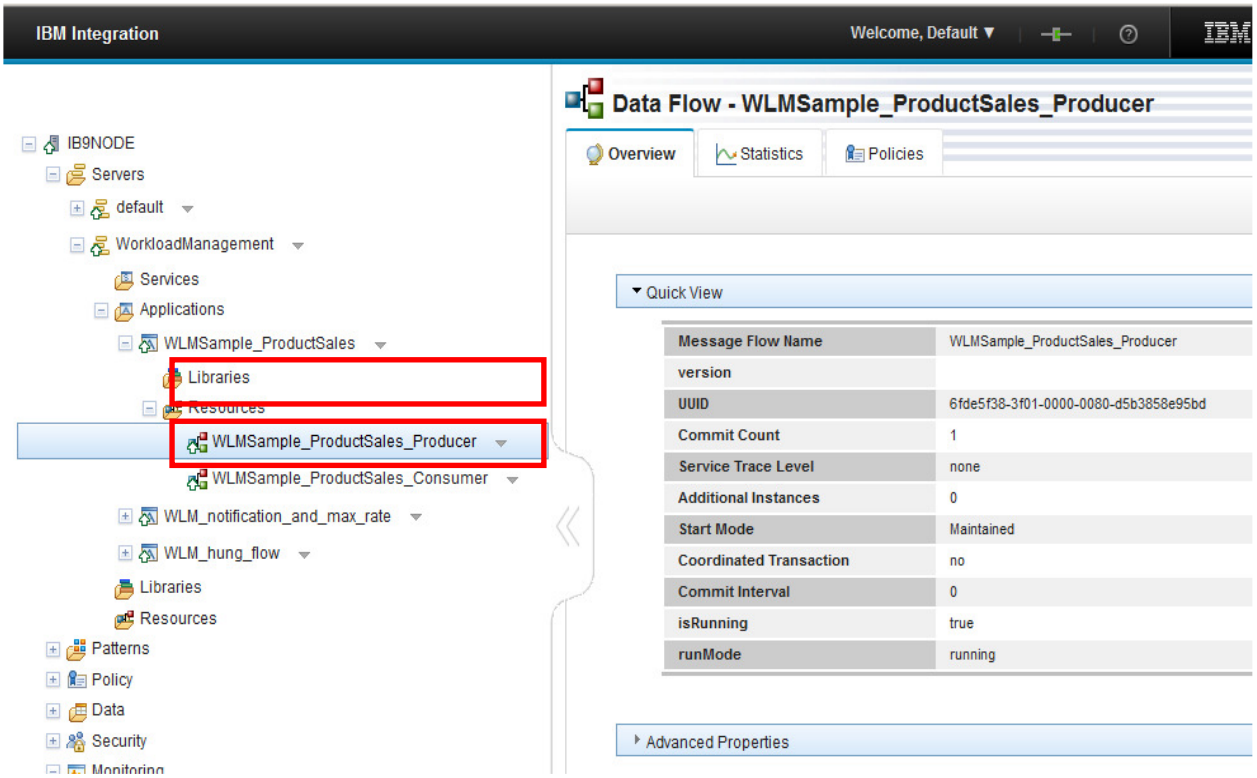


Advanced properties show which traces are on and the default .NET application domain if there is one. Deployed Properties show the barfile name, modified time and date, and the deployed time and date.

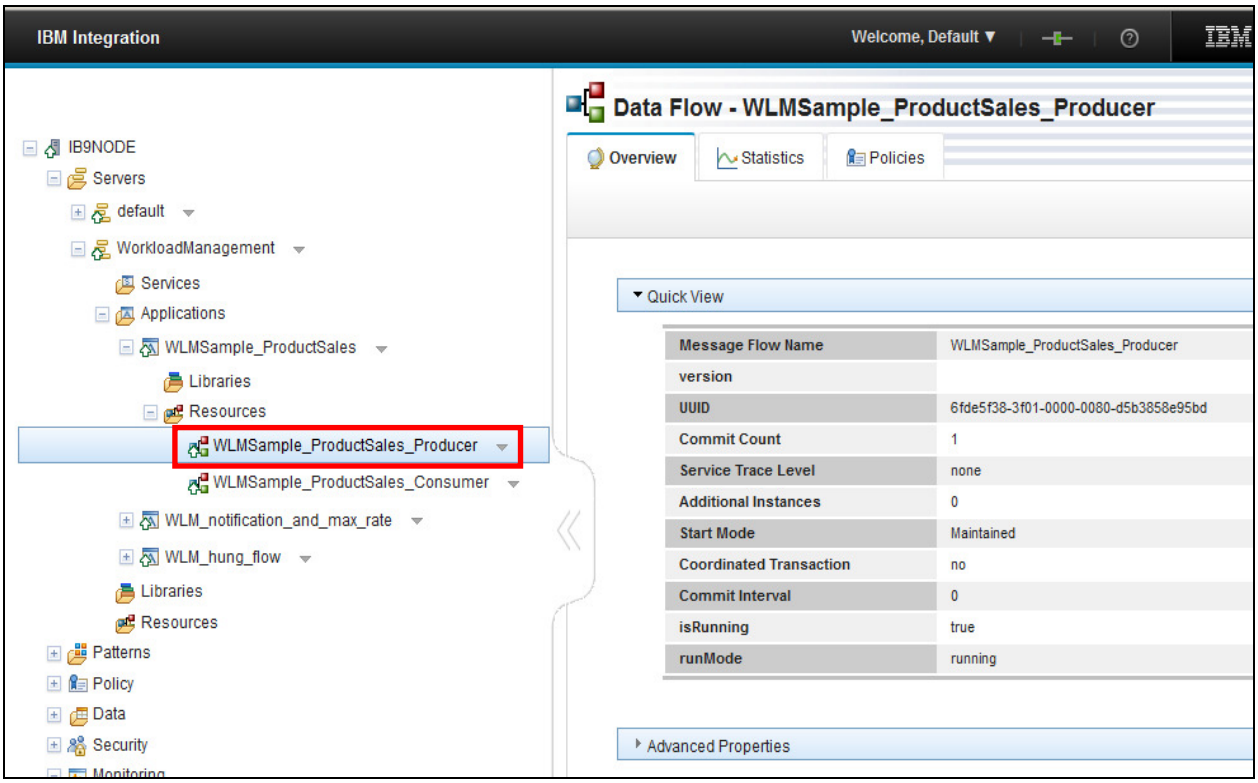
11. Click Statistics. Now you will only see the message flows for the application WLMSample_ProductSales. Again observe that the statistics are off.



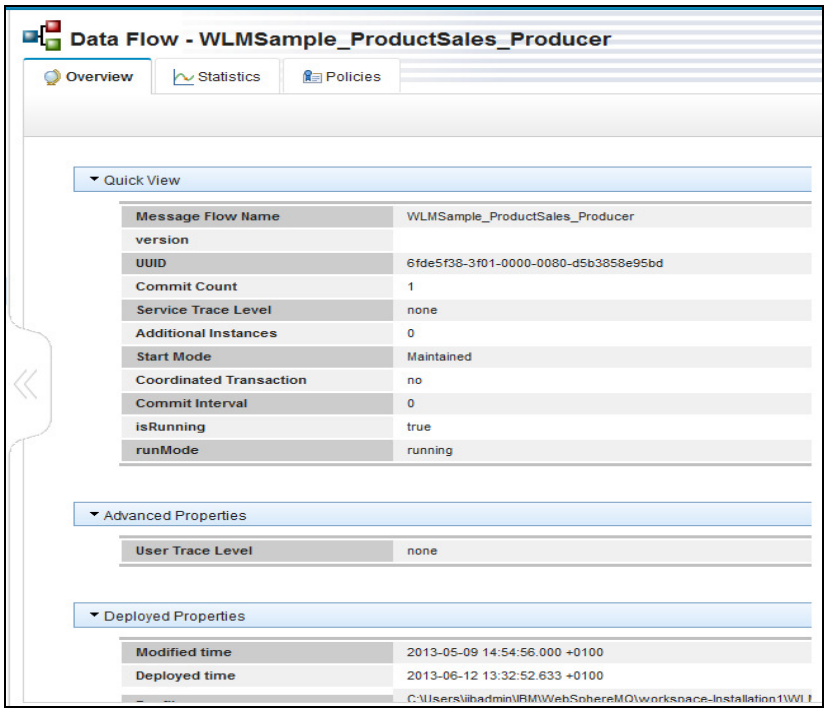
12. Expand the WLMSample_ProductSales application and its Resources where you find the message flows of the application.



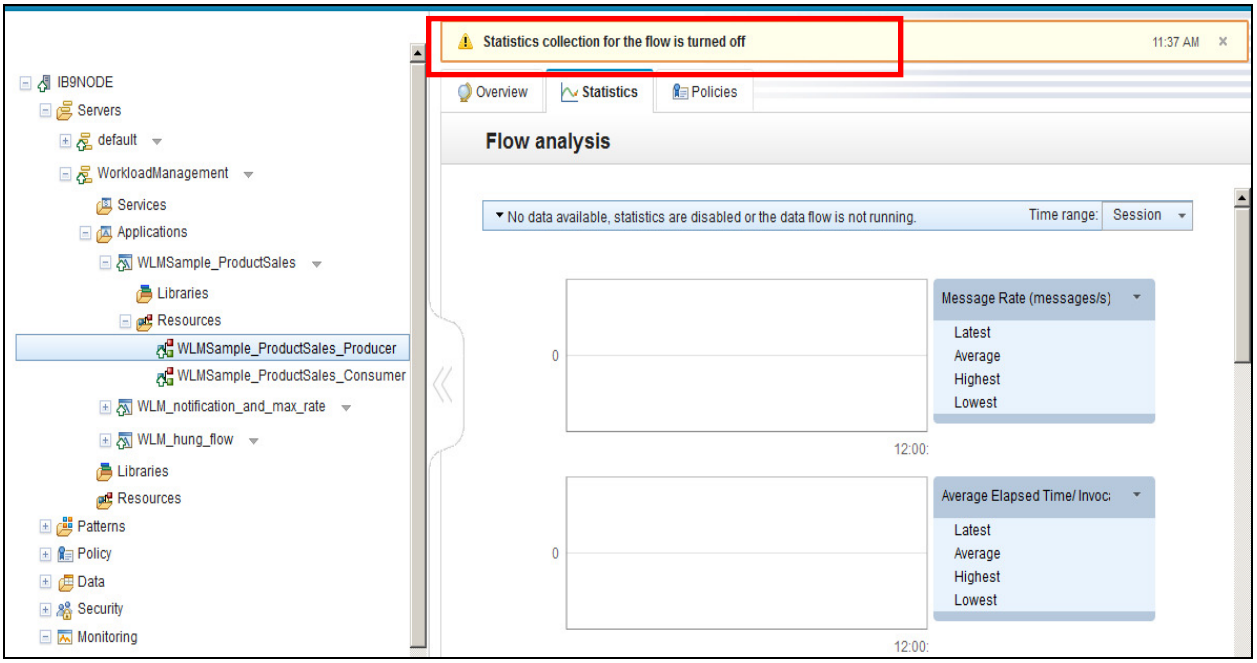
13. Click on WLMSample_ProductSales_Producer. The Quick View shows the common properties of the message flow. The flow should be running.



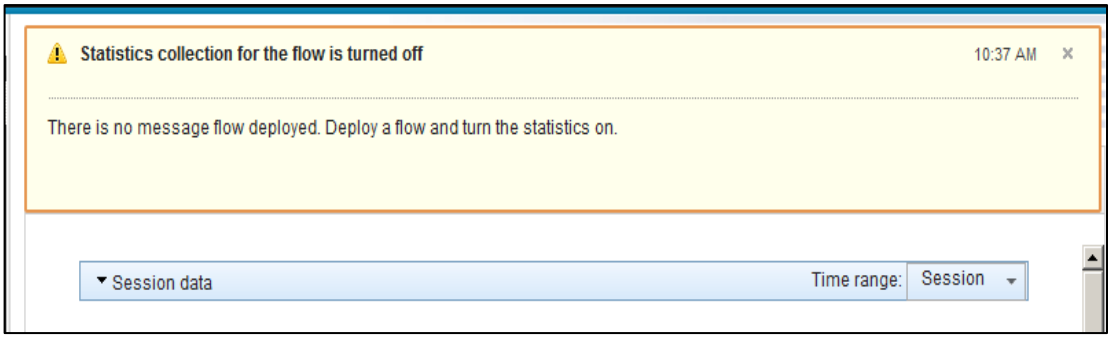
Expand Advanced Properties and Deployed Properties and observe the trace information and deployment information about the flow.



14. Click Statistics. We know statistics are still off and here you see a warning message that they are turned off.
This is the lowest level to turn on statistics. If you only want statistics produced for a particular flow, you need turn on statistics for that flow. If you want statistics for all the flows in an application, you can turn on statistics for the application, and statistics will be collected for all the flows in the application. Likewise you can turn statistics on at the integration server level and all flows in all applications running in the execution group will be collected. And it can be extended up to the integration node level for all flows in the broker. When we do the exercise later in the lab, we will turn on statistics for an application that has two flows running.



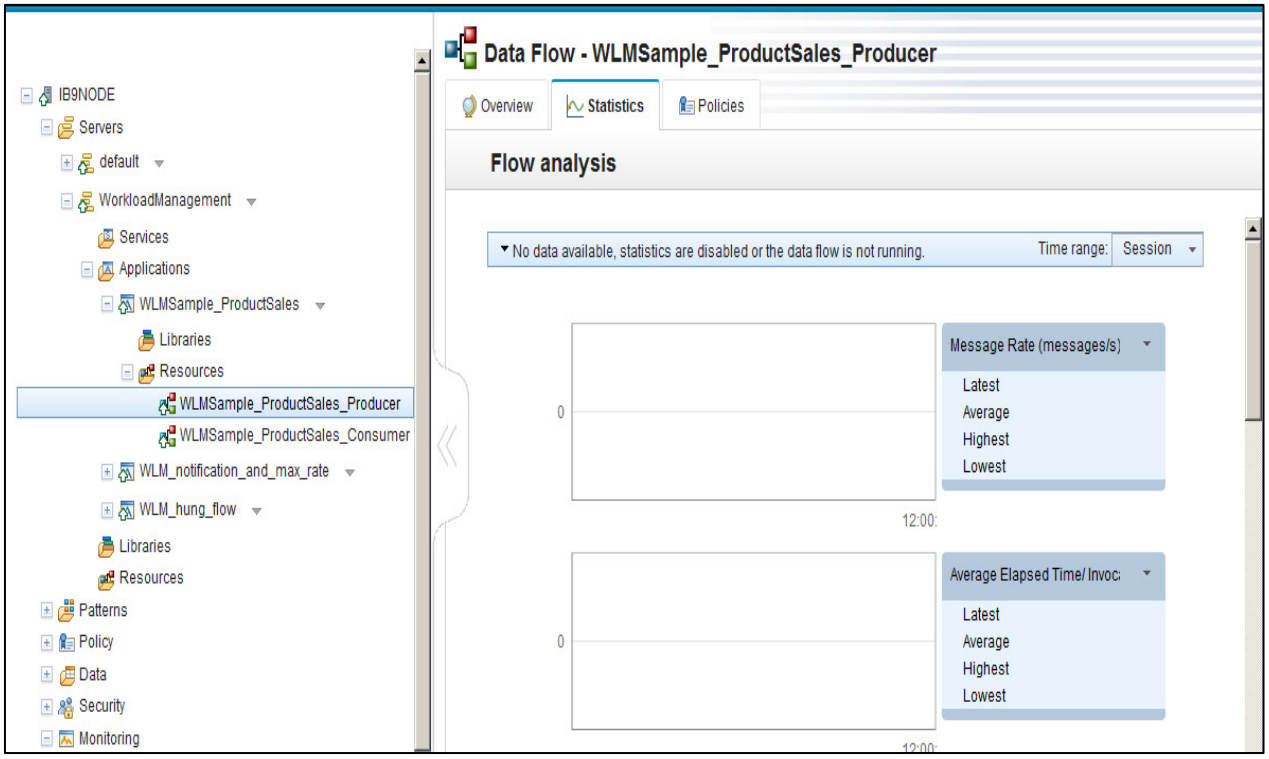
Hover over the message and you will see it is a hyperlink. Click on it and you will see more details about the message if they are available.



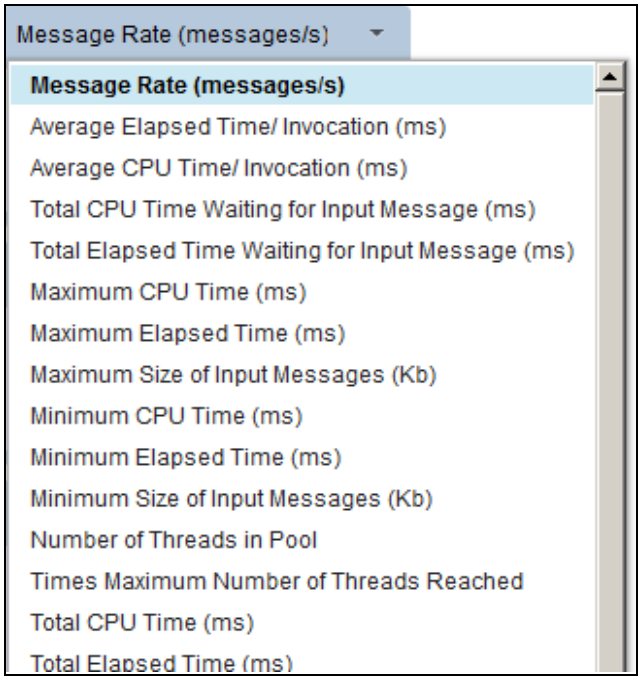
Close the detail popup by clicking the X in the top right corner.

15. In the Web Admin UI, each flow has an area for three graphs to be displayed. The graphs to be shown are determined by the value shown in the title bar of the box. Each box defaults to a particular measurement. You see Message Rate in the first, Average Elapsed Time per Invocation for the second, and Average CPU Time per Invocation for the third. An invocation is the start of a message flow at an input node. It can be an MQInput node, a FileInput, or any other.

    Each box has a pull-down which will show you all measurements which are available.

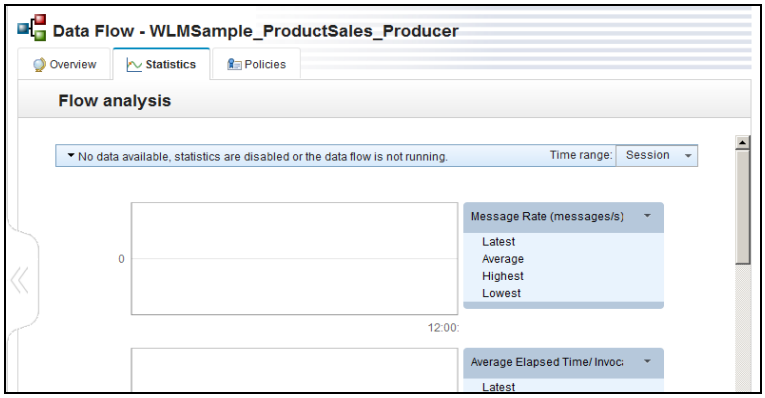


16. Click on the pull-down for the Message Rate box.



The pull-down for each box is the same, so the graphs can be configured to display the measurements you are interested in and in what order.

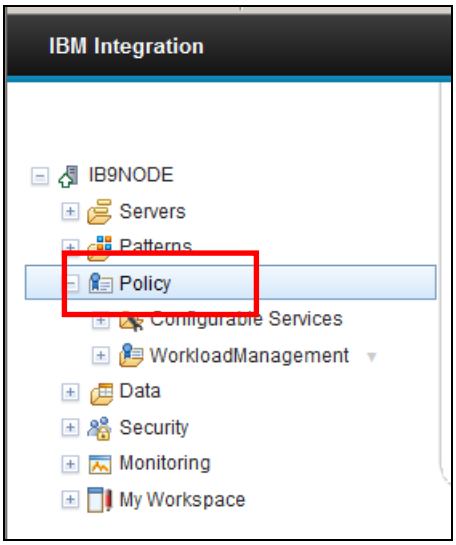
17. In addition, when the flows are running the Latest, Average, Highest and Lowest of the measurement you are graphing will change dynamically as messages are processed. They will change every twenty seconds as that is the snapshot time for displaying the values.



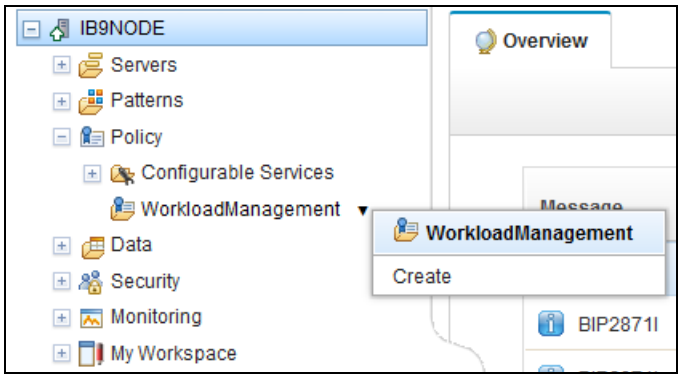
18. Scroll down until you see the Flow Profile category. It should be already expanded. The Flow Profile shows you what nodes are in the flow and how they are connected. There are no details such as node properties, but it gives the administrator an idea of the “flow of the flow” when monitoring statistics.

19. In the web admin navigator, expand Policy.

    Policies are new in IIB V9. Policies can be defined for Configurable Services and for message flows to control Workload Management properties. Once policies are defined, they can be attached to the message flow to control message rates and time-out processing of the flow. Policies are stored in the Integration Node Registry.



20. Expand WorkloadManagement. There are no sub-folders, but you find a drop-down context menu.



    Since there are no policies yet defined, you can only create a policy. Once policies exist, you will be able to select a policy and attach it to a flow.

    You will do that exercise in the next section.

6.2 Using the Web Admin interface to show running flow statistics

Now that you have seen what the Web Admin interface looks like, you will now run some message flows, so that you can view the statistics of running applications and flows.

1. Open three DOS command prompt windows by double-clicking the icon on the desktop.

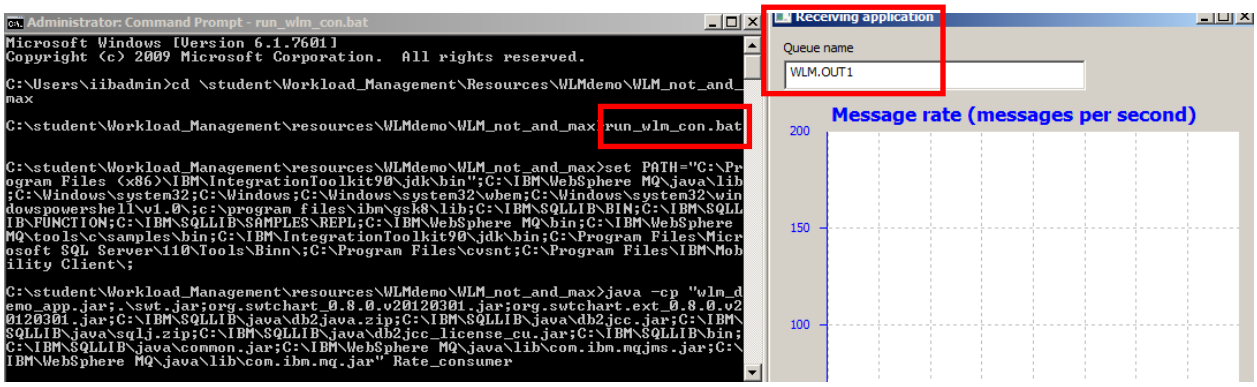
   In each command prompt window, navigate to C:\student\Workload_Management\resources\WLMdemo\WLM_not_and_max.

2. You will run one of three programs in each of the command windows:

   - producer of messages – produces messages as fast as possible
   - consumer of message – can only consume messages at 100 messages / second
   - listener for notification messages – will subscribe to topic string where notifications are published

   Select one window and run the consumer program by entering the following command:

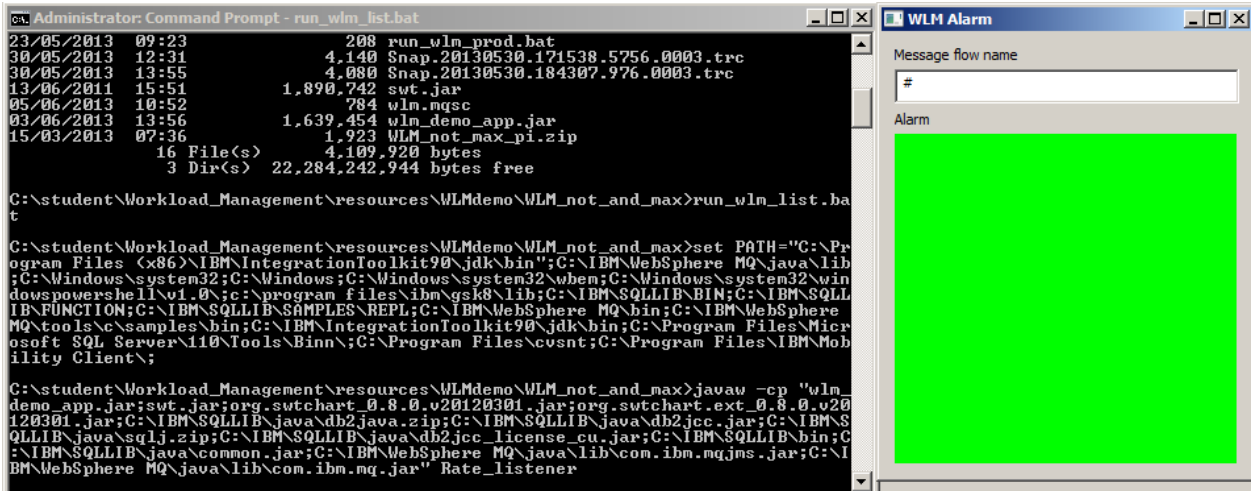
   run_wlm_con.bat



   The application starts up and starts receiving messages on the queue WLM.OUT1 which is the output queue of MQOUTPUT node in the flow which is processing the messages. A running bar graph is displayed showing the message rate at which it is receiving messages. It will send error messages to alert operators that the messages are coming faster than it can handle.

3. In another window, start the listener by typing in the following command:

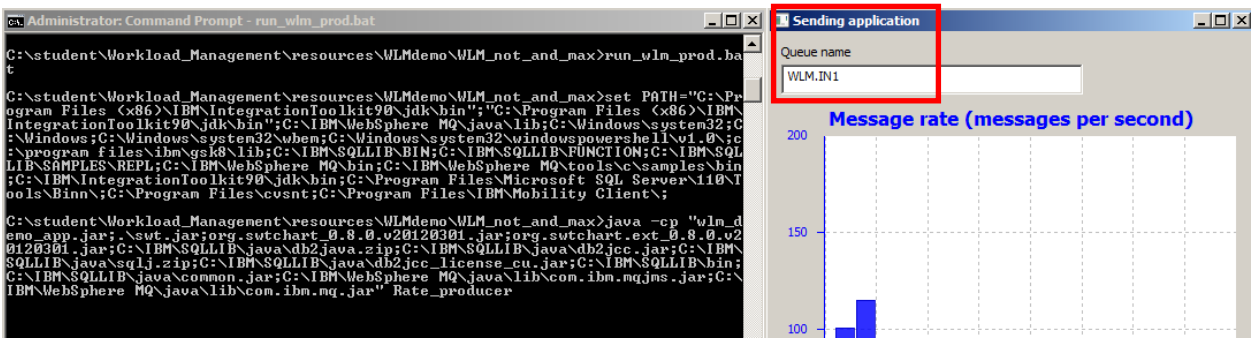
```
run_wlm_list.bat
```



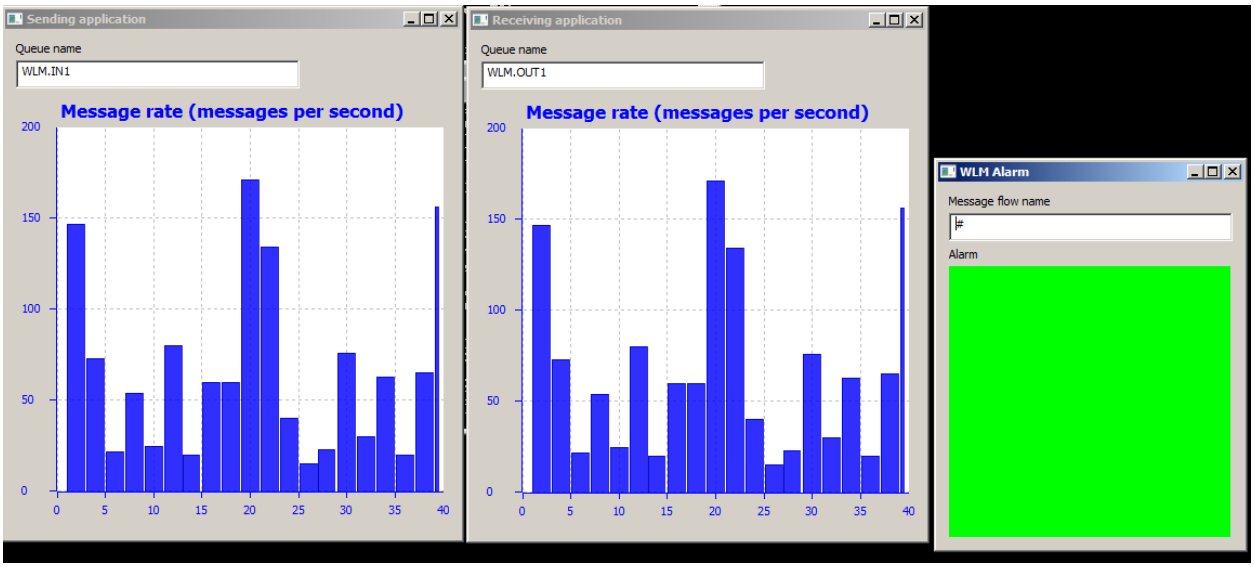
The listener application starts another pop-up window which shows alarms received by the subscription. The application will change the color from green to red if the message rate is too high.

4. In the third window, start the producer program with the following command:

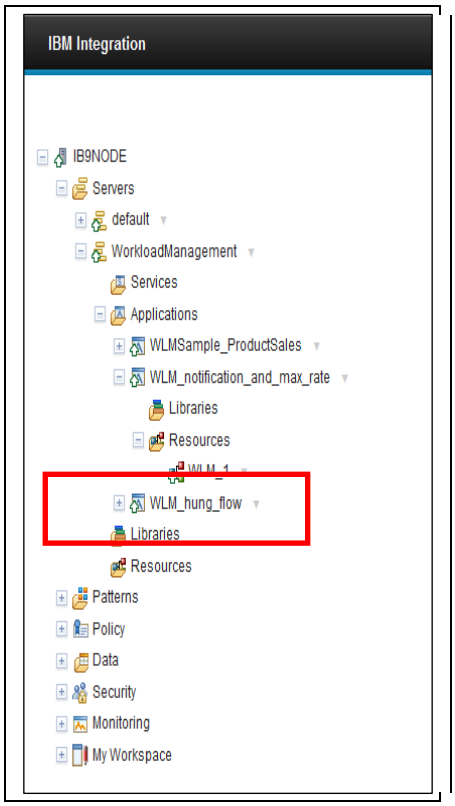
```
run_wlm_prod.bat
```



5. You should now see messages being sent by the producer application and being received by the consumer application. The producer application is putting messages on to the WLM.IN1 queue which is the queue for MQINPUT node of the message flow we will monitor – WLM_1, in the WLM_notification_and max_rate application.

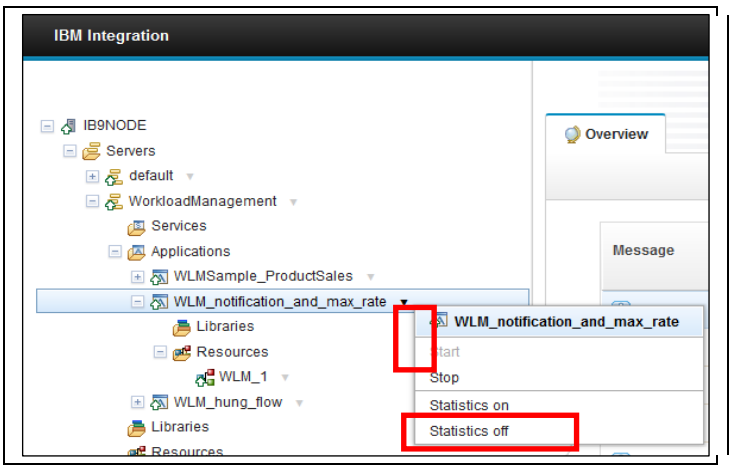


6. Expand the Servers, WorkloadManagement, Applications, and WLM_notification_and_max_rate, and Resources.

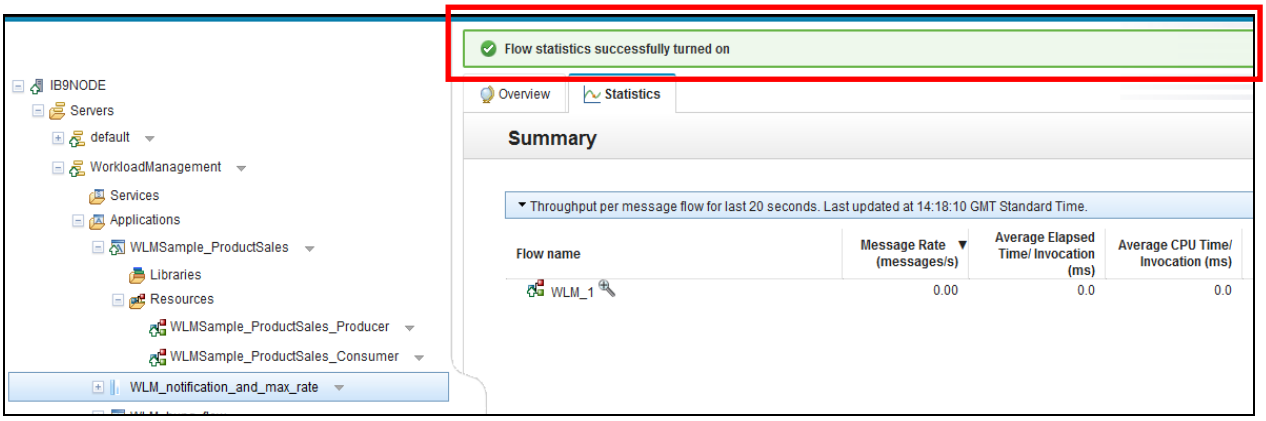


Click the pull-down for the application WLM_notification_and_max_rate.

Select “Statistics on”.



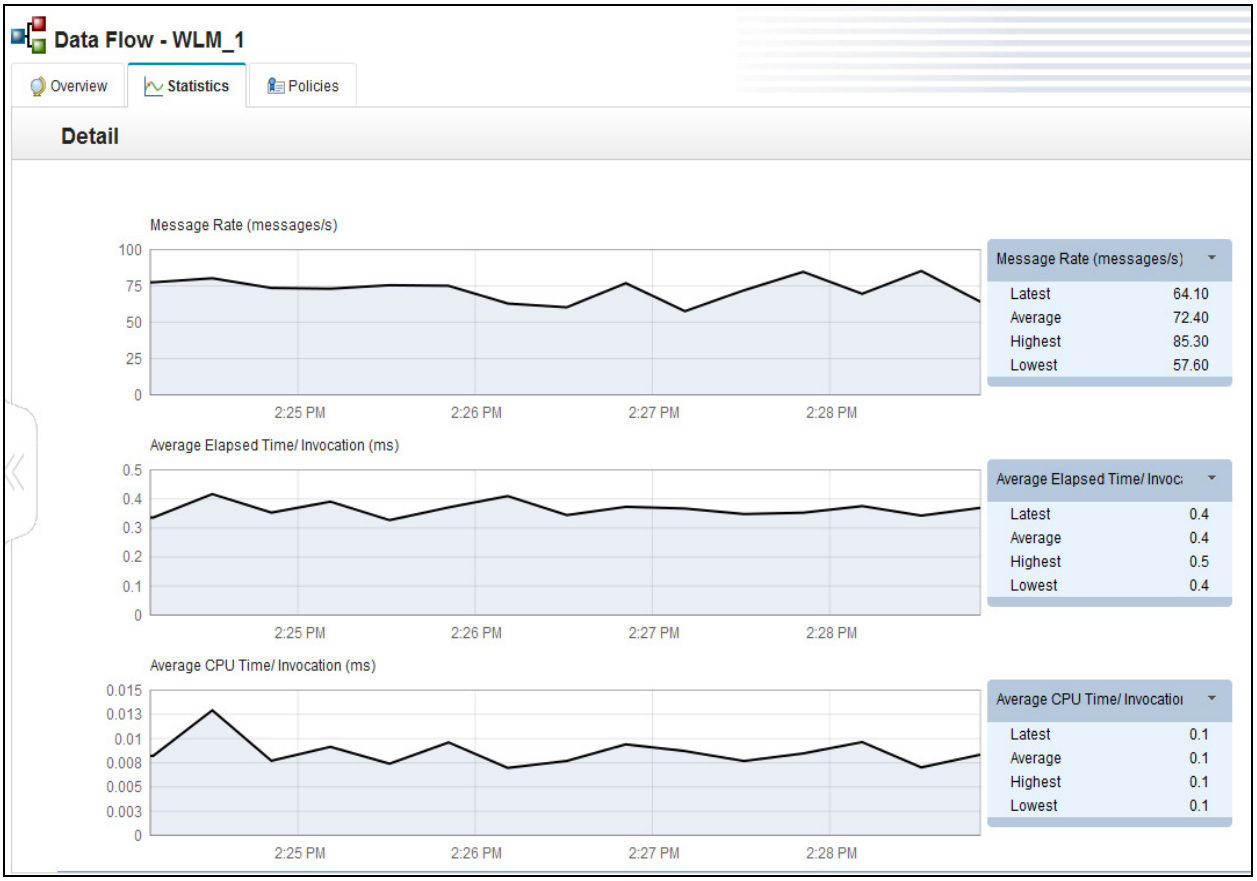
7. You will receive a message that statistics have been turned on. We turned them on at the application level, so statistics for all the flows in the application would be collected. However there is only one flow in this application. We could have just as easily selected the resource WLM_1 and turned on statistics.



8. Click WLM_1. The snapshot interval is twenty seconds, so you will need to wait until the first snapshot has collected the statistics for the period. You will then see the graphs being created.

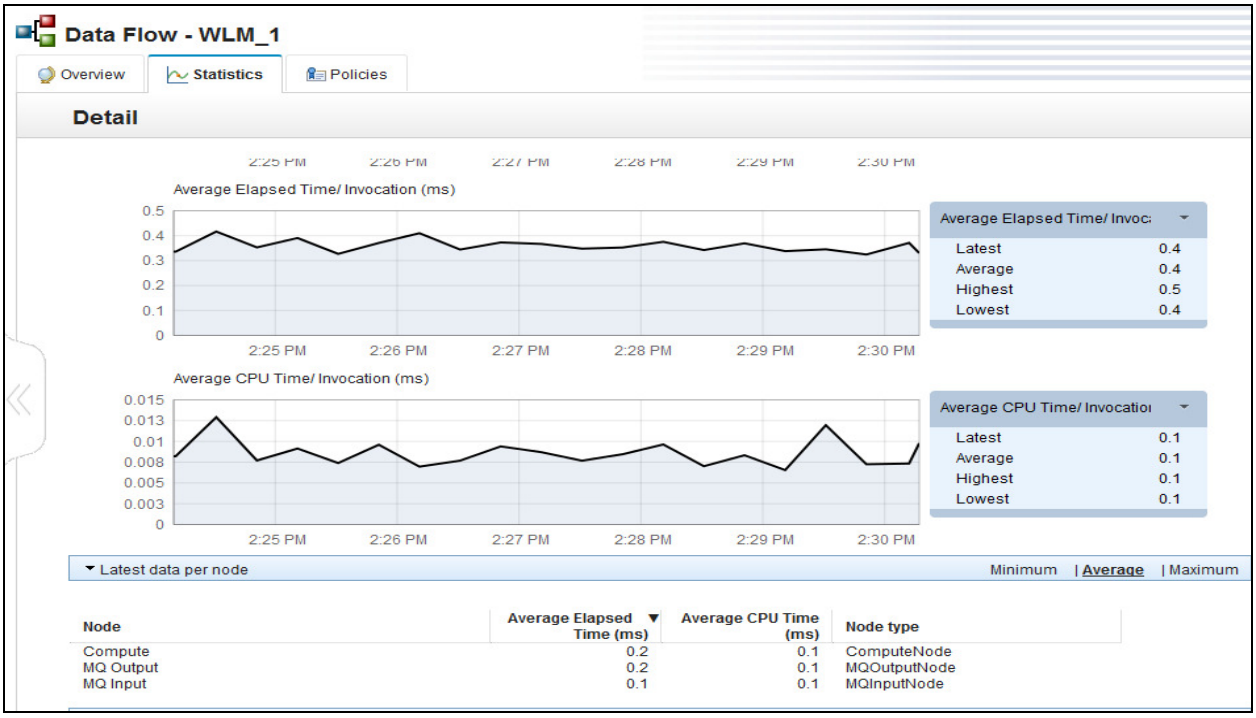
   The time of day is displayed at the bottom of the graph on the x-axis and an appropriate value for the measurement being graphed will be displayed on the left of the graph on the y-axis. Inside the box on the right of the graph you will see the Latest, High, Average, and Low values for the period.

   The graphs are being displayed dynamically, so you can monitor them for a few minutes to see the changes over time.

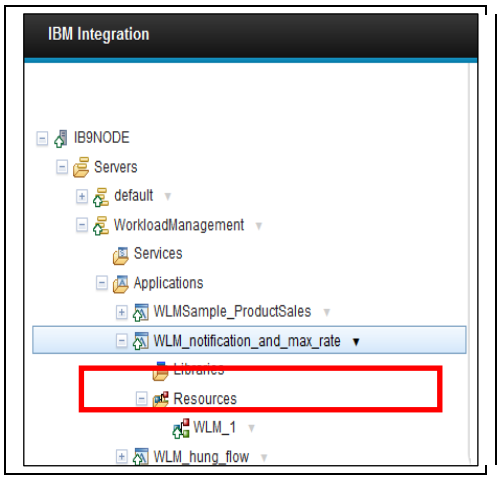


9. Scroll down to the next category “Latest data per node”. Here you will see all the nodes in the flow and the Average CPU Time in milliseconds and Average Elapsed Time in milliseconds. These are the average times which messages spend being processed in that time.

   An administrator can easily see the costly nodes of each flow. As mentioned the Flow profile is the last category displayed. Looking at the nodes in message flow WLM_1, we can see that the time is evenly distributed between all nodes. That’s because it is a very simple flow for demo purposes. The Compute is doing nothing but passing the message through.

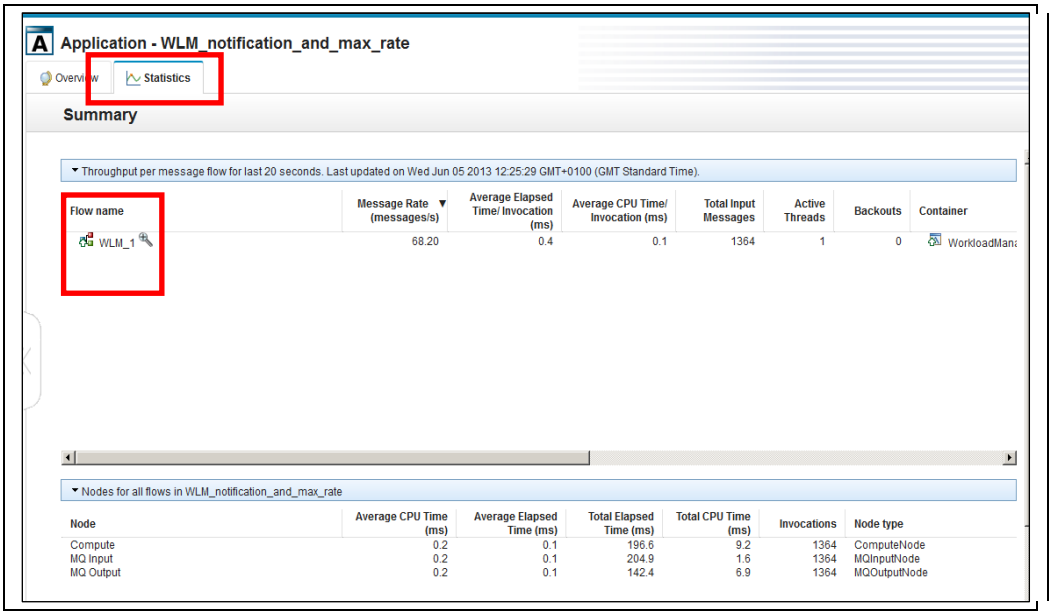


10. Click WLM_notification_and_max_rate application in the navigator.

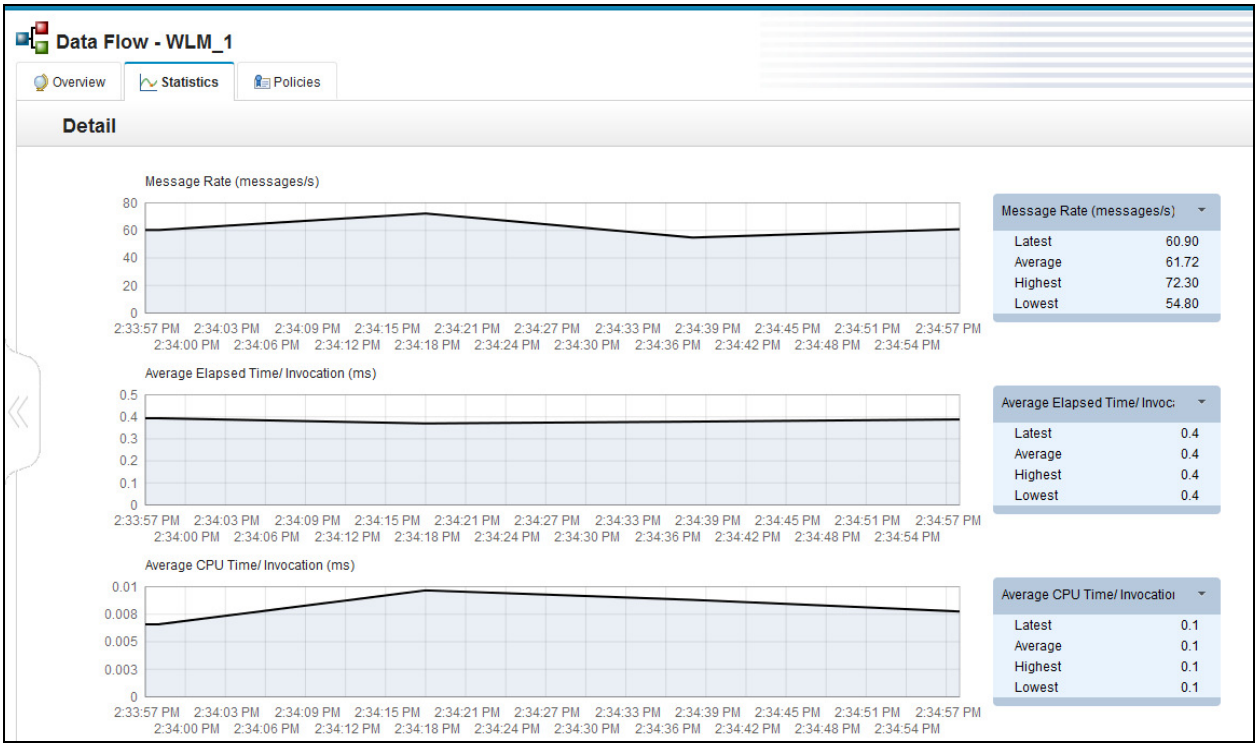


Click the Statistics tab for this flow.

11. Wait for the twenty second interval to pass. You will see all the flows which are running in the this application (only WLM_1).
You may need to scroll to the right or adjust the navigator bar to see all of the columns. Notice the title of the columns. They are the measurements you saw in the pull-down menu for the graphs earlier.



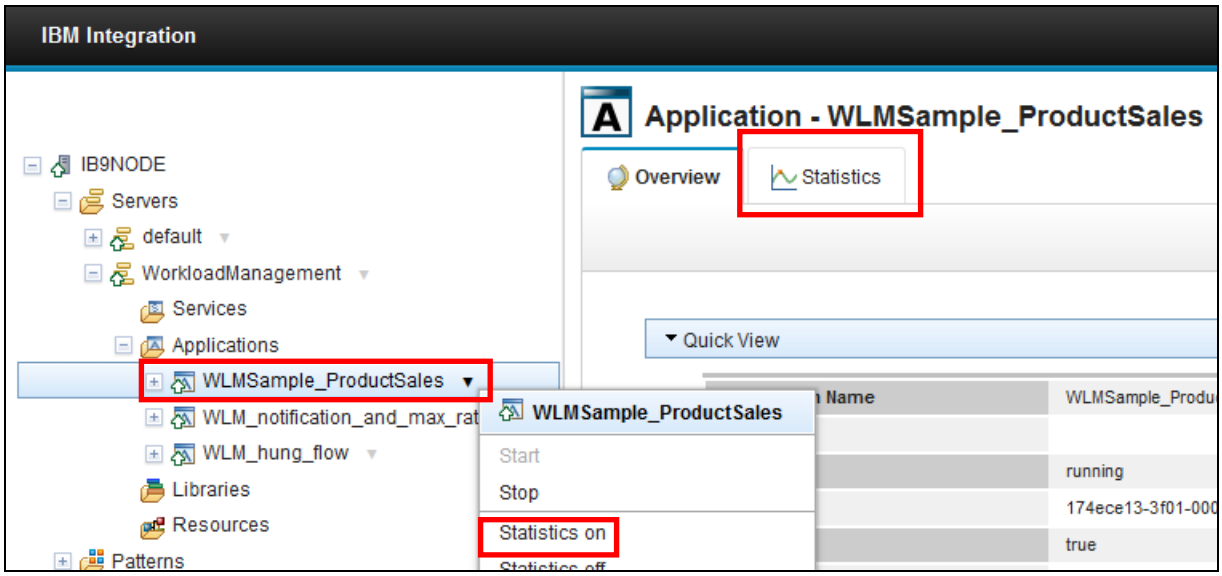
12. After the twenty second interval, you will see a small magnifying glass next to the flow name. Click the magnifying glass icon and the detailed graphs will be displayed for that flow.



13. As mentioned earlier, you can do the same at the Integration Server and Integration Node levels.

    Remember, once statistics are set on for the flow, you do not need to do it at the higher levels. Manipulating statistics at the higher level, sets them on or off for all flows within that container. Try that now.

    Click WLMSample_ProductSales to bring it into view. Set statistics on for the application.

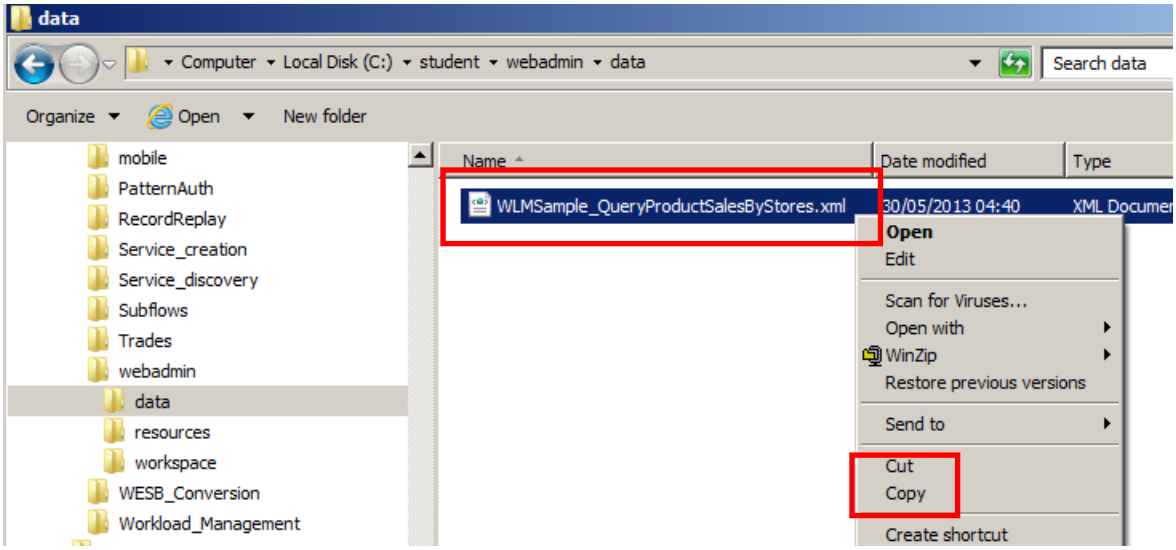


    Click the Statistics tab.

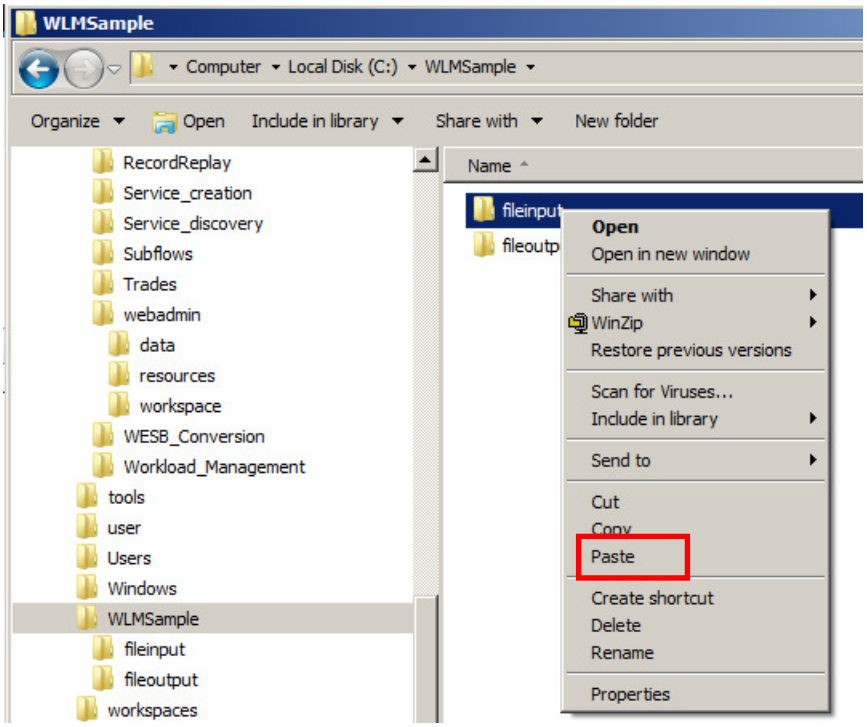
14. Send data to the flows.
    In an Integration Console 9.0 session, navigate to C:\student\webadmin\run\Run_slow_tcpip_app. Enter the command *slow_tcpip_app*.

    This application simulates a slow back-end application that is being flooded by messages from the integration bus. You will slow down the message rate sent to this application by creating a policy in the integration bus, and applying it to the particular integration application.

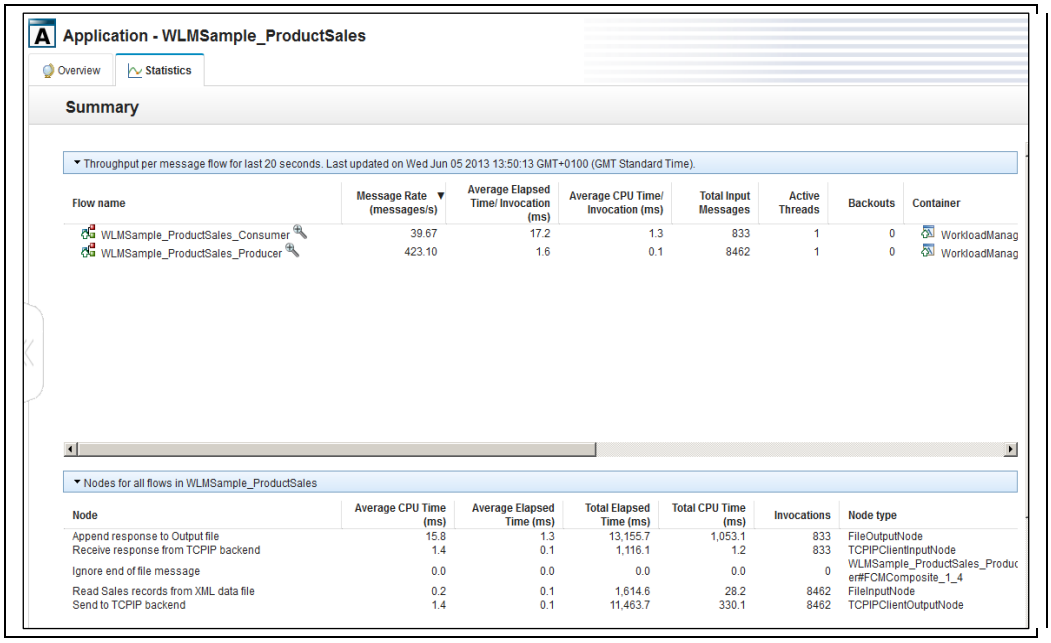
15. In a Windows Explorer window, navigate to C:\student\webadmin\data. Right click the WLMSample_QueryProductSalesByStores.xml file and select Copy. (This file contains a large number of records).



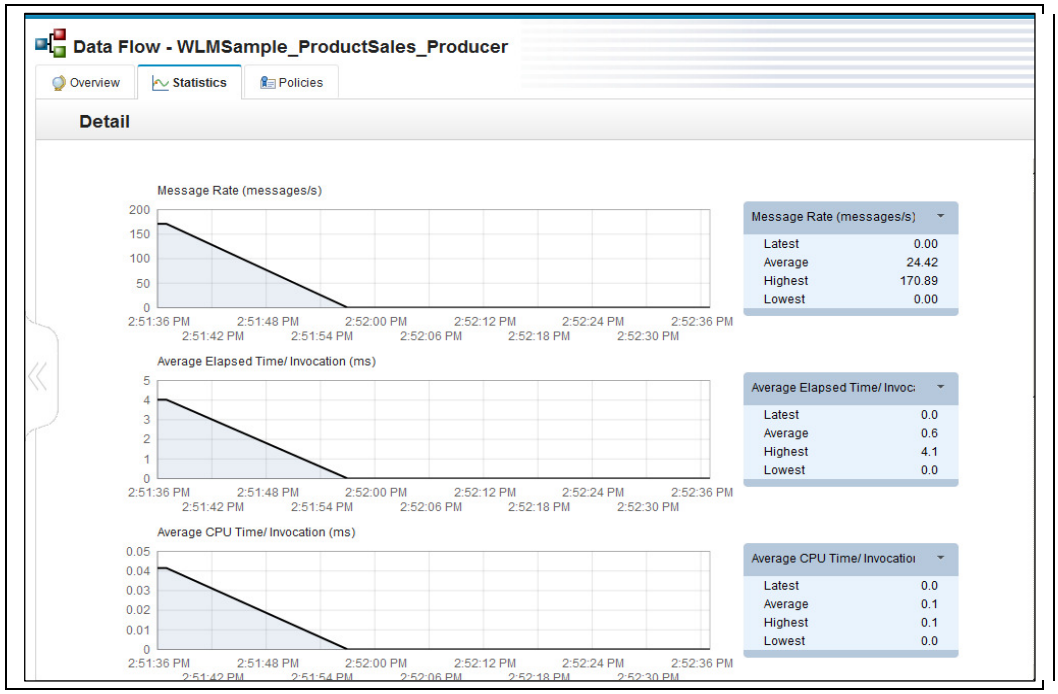
Navigate to C:\WLMSample and paste this file onto the fileinput directory.



16. Return to the browser window and wait for the screen to refresh. You will now see the statistics displayed for both flows in the application.

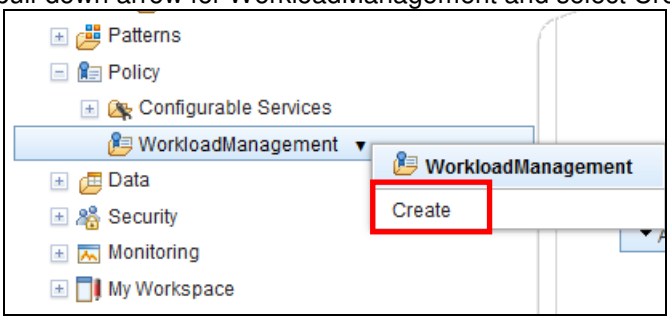


17. Click the WLMSample_ProductSales_Consumer flow to see the detail graphs for the flow.
This application will run quickly, so you may see a declining rate like this. If you are too late, just rerun the application by copying the data file again and pasting into the C:\WLMSample\fileinput directory.

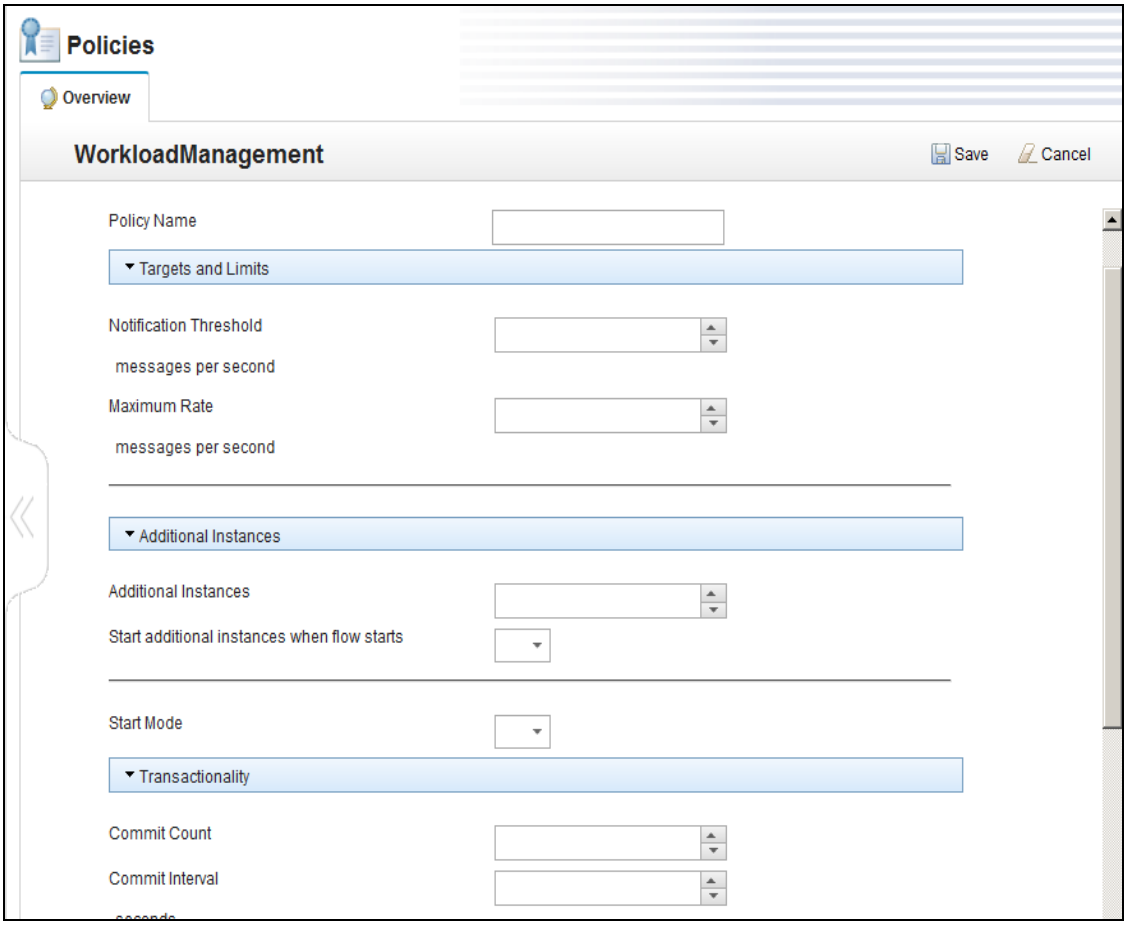


6.3 Create and use a policy to limit flow throughput

1. Expand Policy. Click the pull-down arrow for WorkloadManagement and select Create.



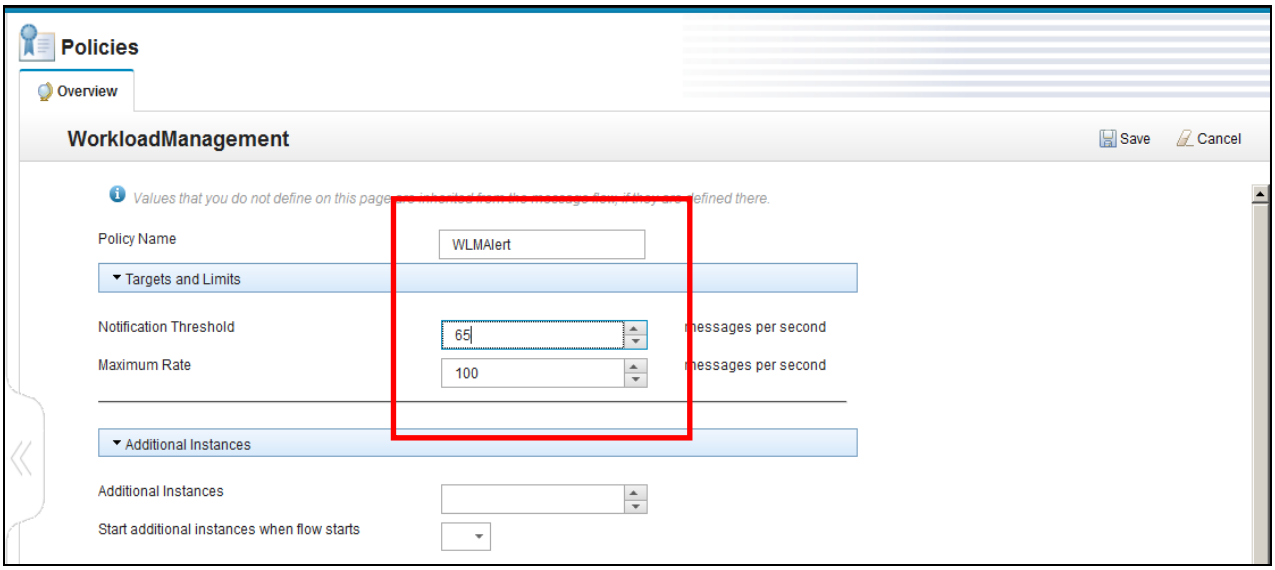
2. The WorkloadManagement properties are displayed.



Notice that they are divided into four groups (scroll down to see all four); Targets and Limits, Additional Instances, Transactionality, and Unresponsive Message Flows. Review the groups and properties. This is the way in which the WebAdmin UI presents the properties, in logical groups. The IB Toolkit only lists the properties in the message flow editor.

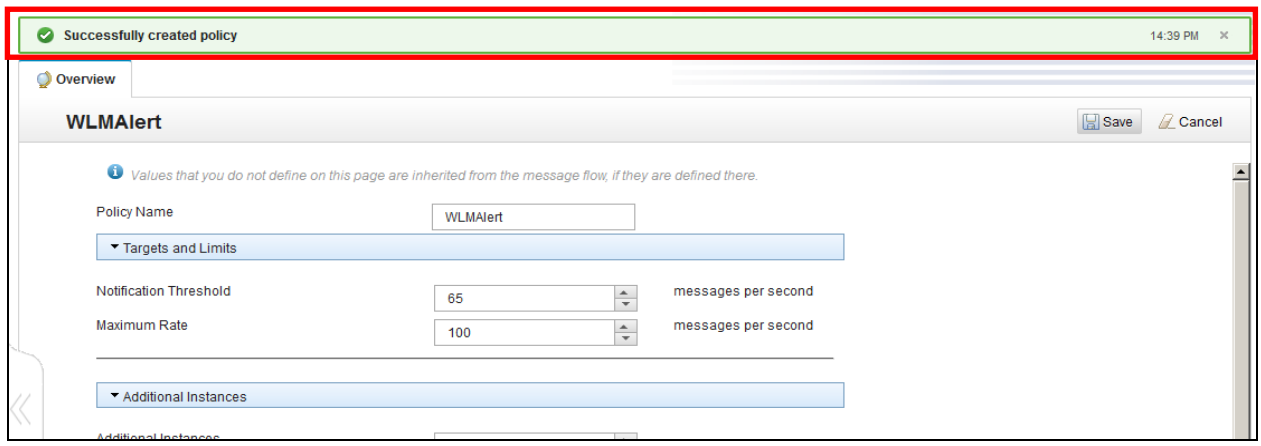
You can collapse Additional Instances and Transactionality as we will only create policies for Targets and Limits and Unresponsive Message Flows.

3. In Policy Name, type WLMAlert. Set the value for Notification Threshold to 65. Also set the maximum message rate to 100.

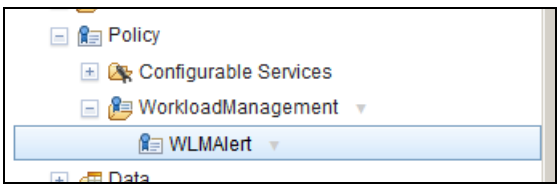


Click Save (this may take a few seconds to save and refresh the navigator).

4. You will get a confirmation that the policy was successfully created.

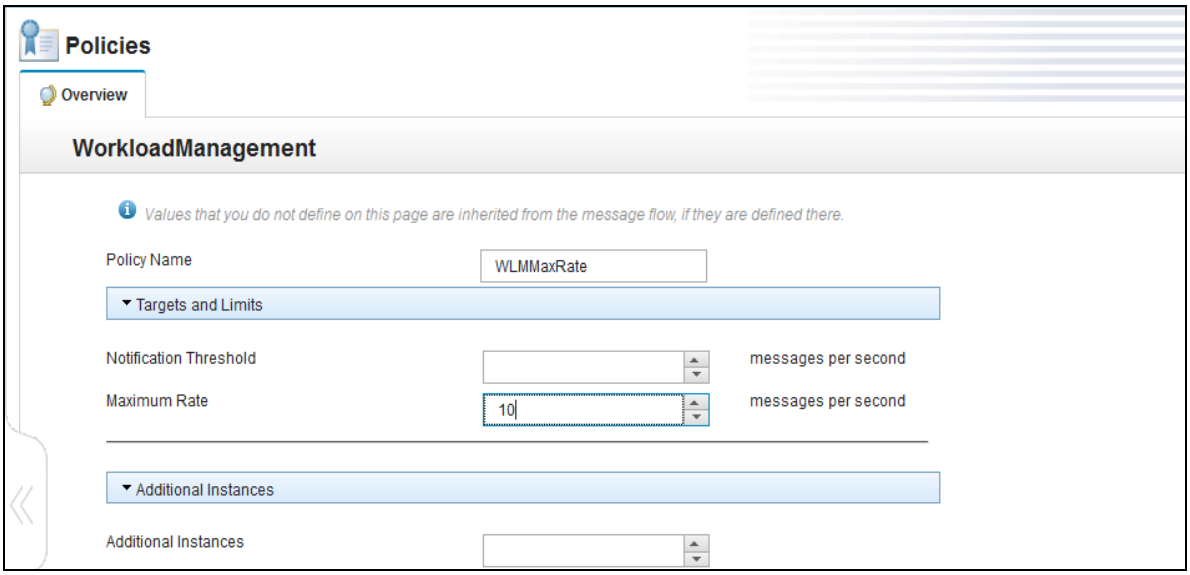


You will see the new policy WLMAlert under the Policy > WorkloadManagement folder.



5. Create another policy. Click on the WorkloadManagement pull-down and select Create. Name this policy WLMMaxRate.

   Set the Maximum Rate to 10.

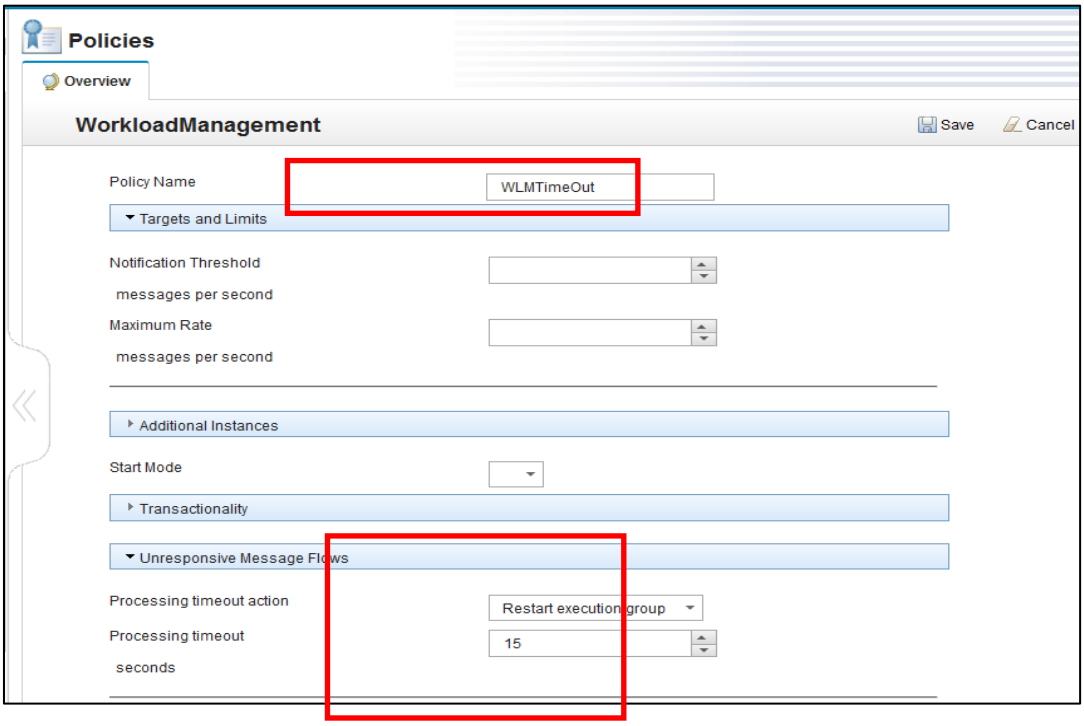


   Click Save and wait for the success message. (this may take a few seconds to save and refresh the navigator)

6. Create one more policy called WLMTimeOut. Collapse all the groups except Unresponsive Message Flows.

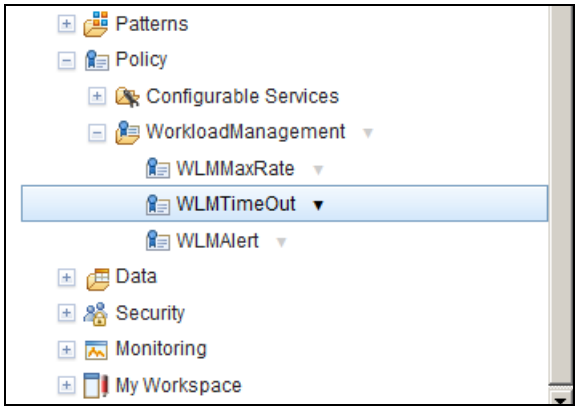
   Click the pull-down for Processing timeout action and select “Restart execution group”.
   Type in 15 for the Processing timeout.

   This policy will not be used during this lab but is highlighted to show that a policy can be used to control the unresponsive behaviour of a message flow. For more information with regards to unresponsive flows please see the lab guide 'WorkloadManagement Unresponsive Flows'.

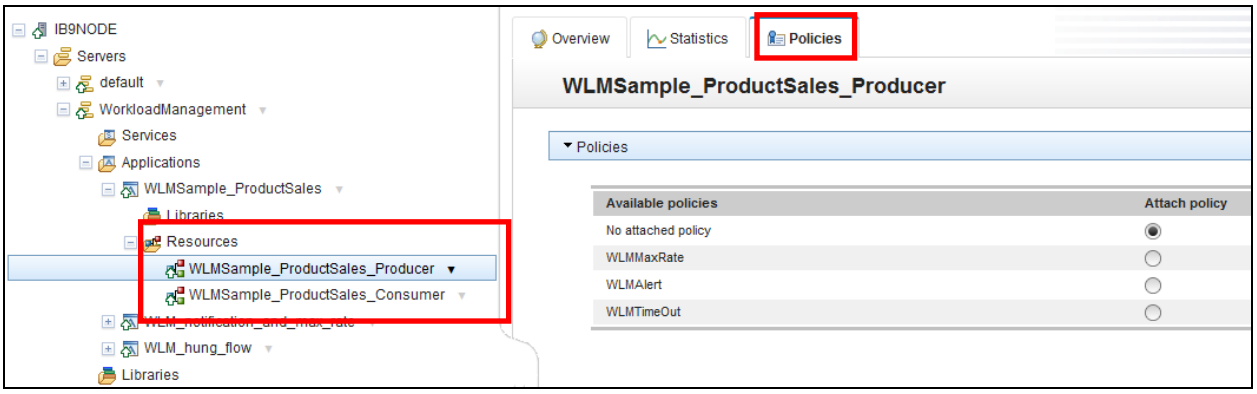


   Click Save and wait for the success message. (this may take a few seconds to save and refresh the navigator)

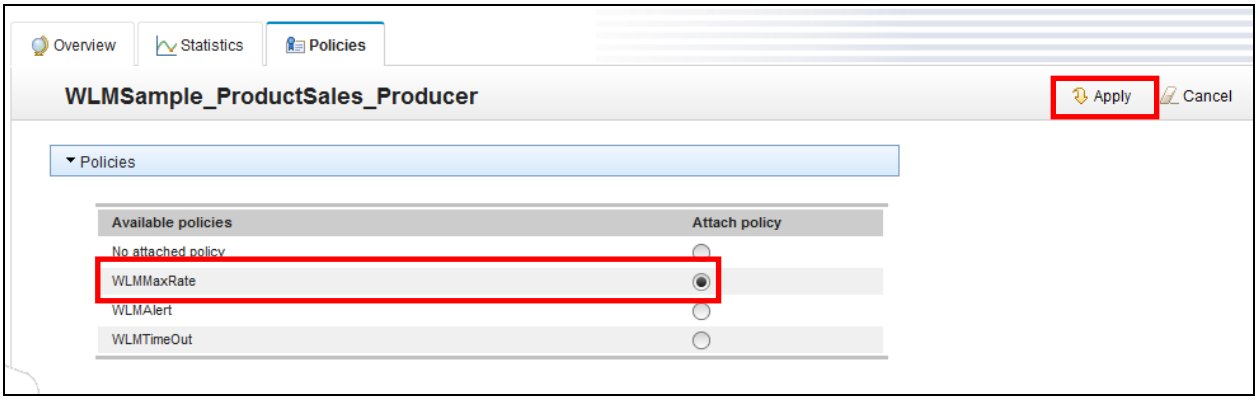
7. You now have three policies.



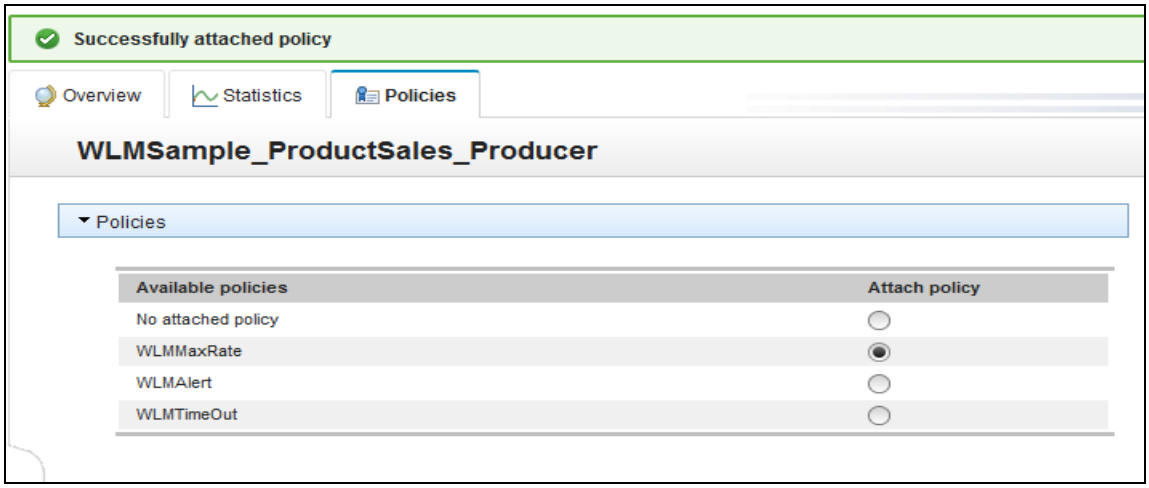
8. Click the WLMSample_ProductSales_Produce message flow under WMSample_ProductSales > Resources.



The WLMSample_ProductSales_Consumer message flow can only handle ten messages per second. So we need to throttle the WLMSample_ProductSales_Consumer flow to only send ten messages per second. We now have a policy, WLMMaxRate, that specifies a maximum message rate of ten messages per second.
To accomplish this, we can attach WLMMaxRate policy to the WLMSample_ProductSales_Producer message flow.
Click the radio button for WLMMaxRate. Then click Apply.

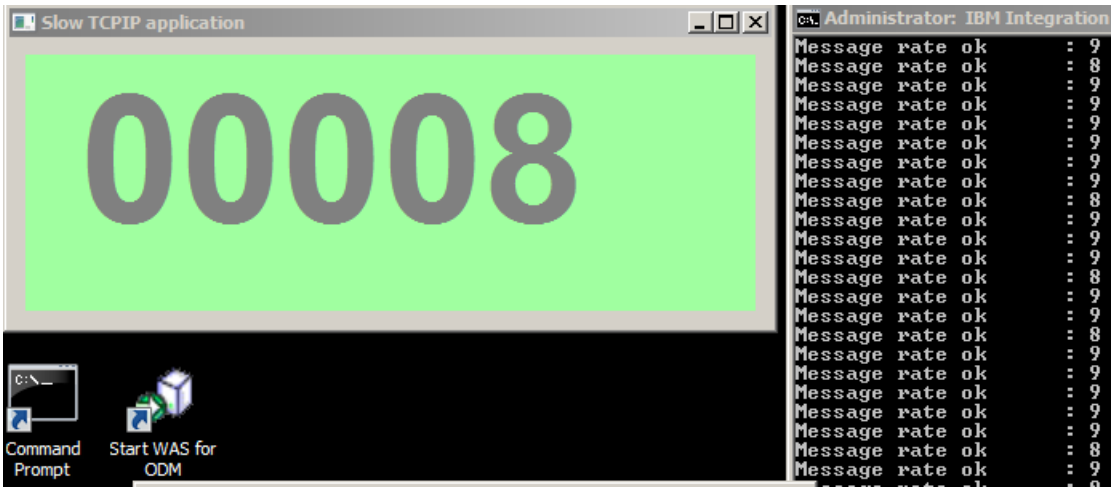


You will receive a completion message. (This may take a few seconds)



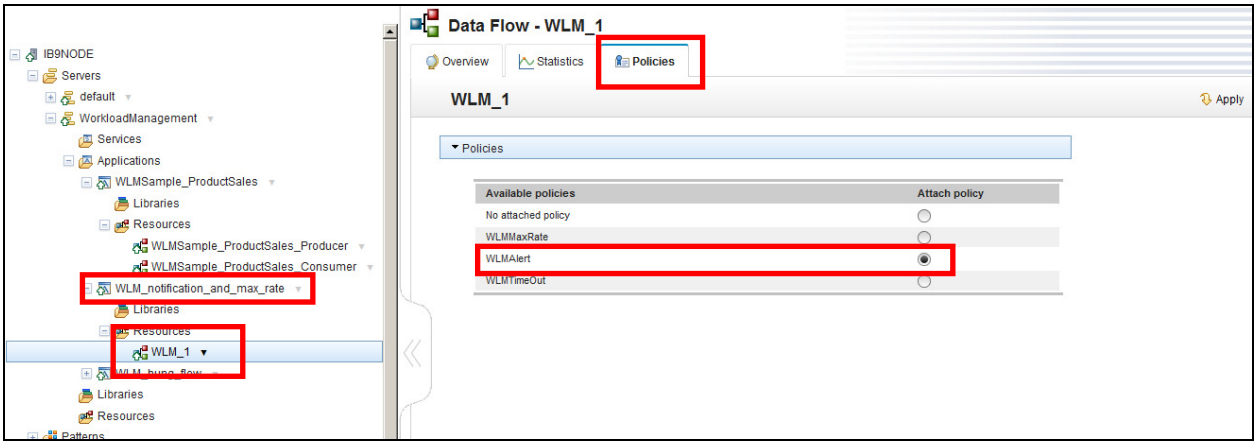
9. Repeat steps 15 and 16, from the previous section, to rerun the WLMSample_ProductSales application.

   Bring the Slow TCPIP application monitor into view and observe that the message rate never exceeds ten messages per second which is what the policy WLMMaxRate enforces.



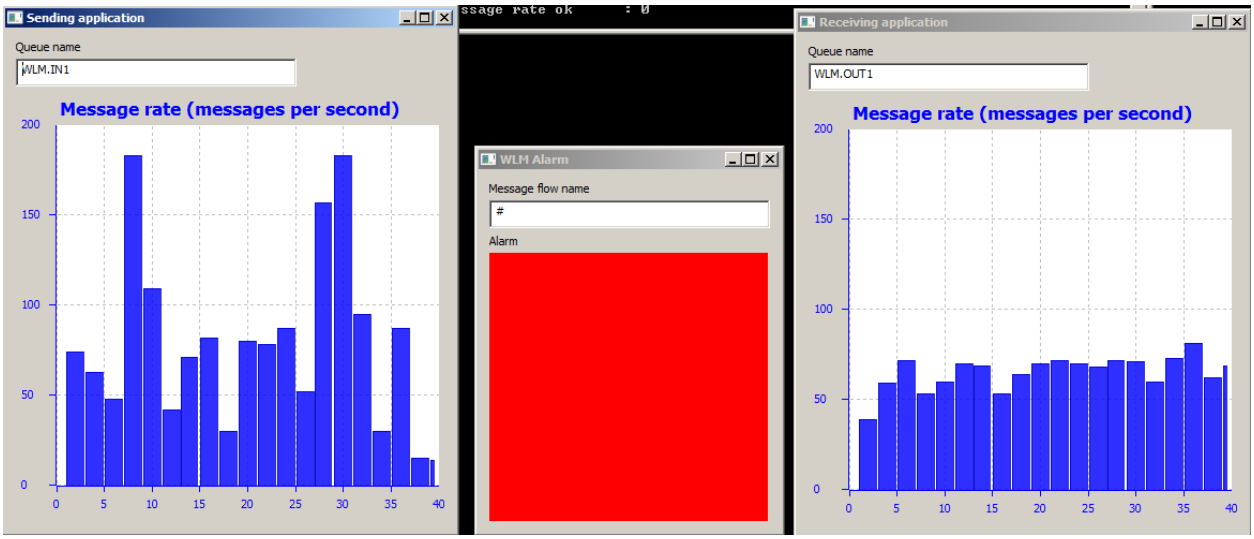
   If you didn't notice, there was no re-deploy of the application necessary to put the policy into effect. All that was needed was for the administrator to attach the policy to the message flow and the WebAdmin tool dynamically enforces the policy on the flow by automatically doing the redeploy.

10. Now attach the WLMAlert policy,click apply to the WLM_1 message flow in the WLM_notification_and_max_rate application.



   Don't forget to click Apply. You will receive a completion message. 'Successfully attached policy'. (This may take a few seconds)

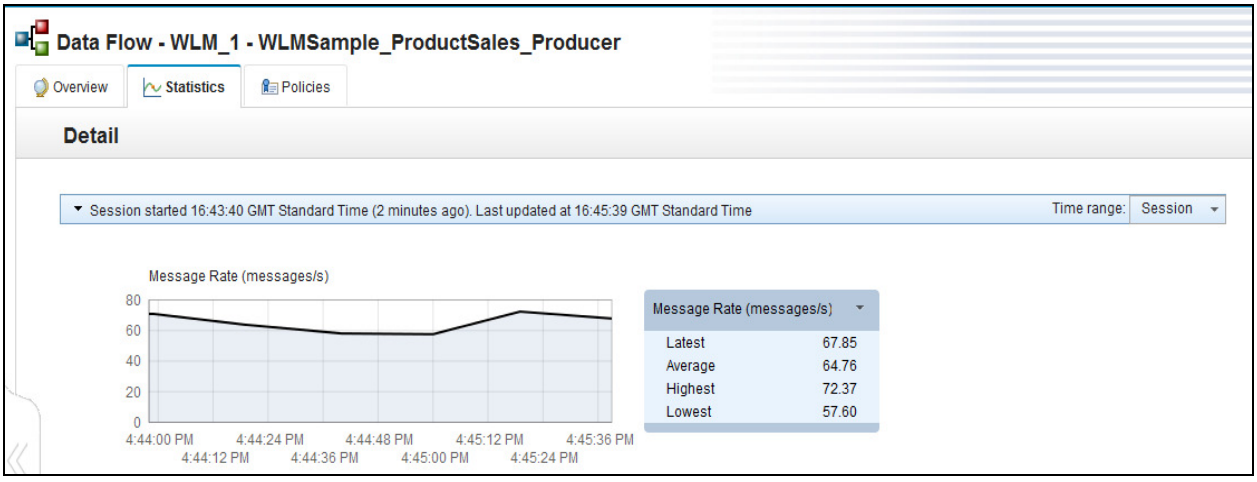
11. Bring the WLM Alarm, Sending application, and Receiving application windows into focus and observe the effect of the policy.



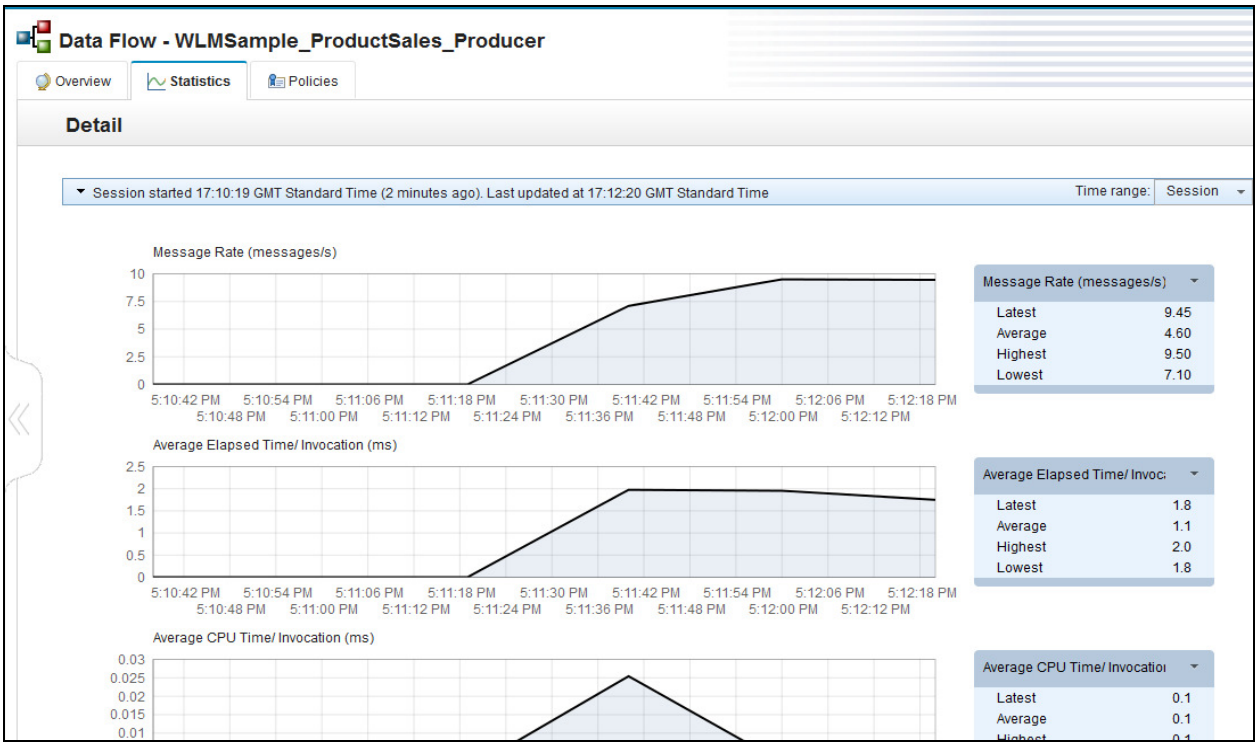
Monitor the WLM Alarm window for a few minutes. You should see it change from green to red to green as the message rate goes above and below the sixty-five messages per second rate defined in the WLMAlert policy. You should see the effect of the message rate on the Receiving application immediately. The graph has smoothed out and is under 100 messages per second. Again, the policy only needed to be attached to the flow, IIB WebAdmin did the rest.

12. Return to the web browser session and see if you can correlate what you have observed with the statistics in the WebAdmin.

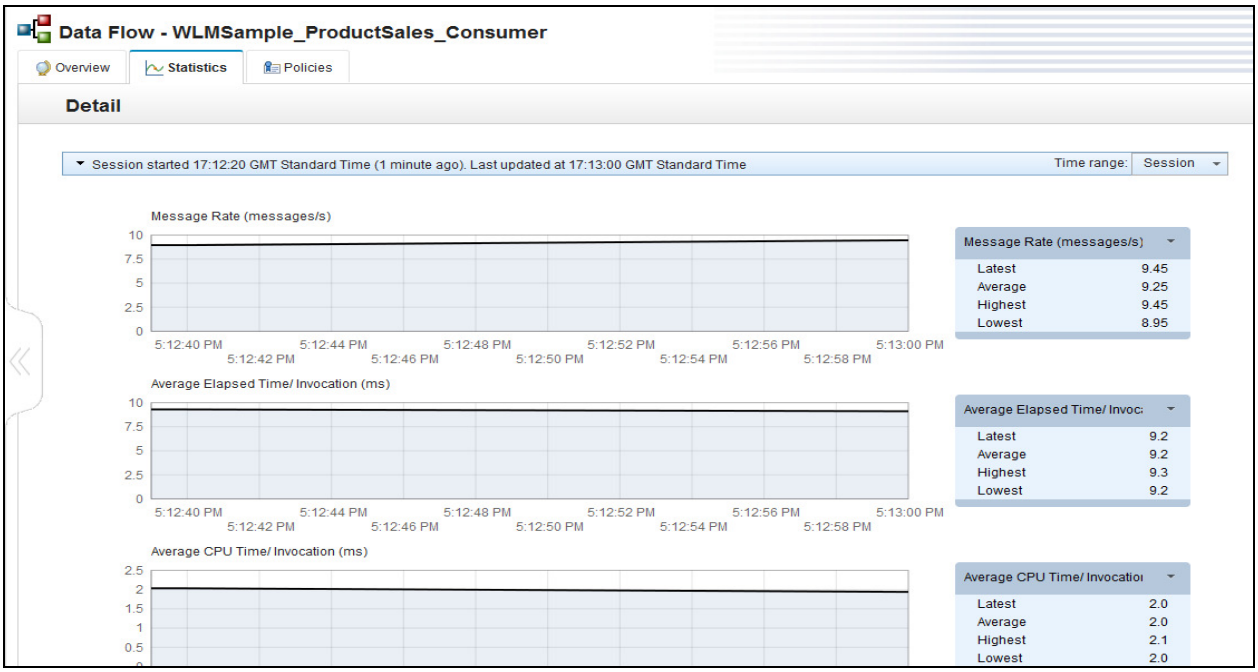
Obviously, we want to look at the message rate WLM_1. It should be that the flow is definitely producing messages well under the rate of one hundred set in the policy. You can also see the its high was over seventy and thus the red alarm.



13. Click the WLMSample_ProductSales_Producer flow. We should not see the rate go above ten. This screen shot was taken as the application started sending messages, so you can see the rate gearing up from zero to just under ten which is exactly what the WorkloadManagement policy was intended to do. If you completed the WorkloadManagement Throughput Control lab, you know this application sent messages as fast as it could, over three hundred messages per second, without any throttling.



14. Have a look at the consumer flow also before you close the windows. Since this is the back-end application, we would not attach a policy here (unless it may be producing messages for another application). This is the application we are protecting with a WorkloadManagement policy and the fastest it can process messages is ten per second. It appears the application should be happy, because it is processing just under ten messages per second.



This concludes the Web Admin lab. You can see that the Web Admin browser interface is a very friendly and functional tool for IIB administrators. Message flows can be monitored and policies can be configured and attached to those flows to control workload for backend applications.